INTERNATIONAL STANDARD

ISO/IEC 10021-8

First edition
1995-08-01

Information technology — Message Handling Systems (MHS) —

Part 8:
Electronic Data Interchange Messaging Service

Technologies de l'information — Systèmes de messagerie (MHS) — Partie 8: Service de messagerie avec échange de données informatisé

Reference number
ISO/IEC 10021-8:1995(E)

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Definitions 2
3.1 Terms defined in this part of ISO/IEC 10021 2
3.1.1 EDI forwarding 2
3.1.2 EDI message 2
3.1.3 EDI messaging user 2
3.1.4 EDI notification 2
3.1.5 EDI message responsibility 2
3.2 Terms imported from ISO/IEC 9735 3
3.3 Terms imported from ANSI X12 3
4 Abbreviations 4
5 Conventions 4
6 EDI messaging service 5
6.1 Introduction 5
6.2 EDI messaging 5
6.3 EDI messaging environment 5
6.4 EDI messaging user 6
7 EDI messaging system 6
7.1 Introduction 6
7.2 Information flow in the EDIMS 7
7.3 EDI messaging service functional model 8
7.4 Structure of EDI messages 9
7.5 EDI notification 11
8 EDIM responsibility and forwarding 11
8.1 Introduction 11
8.2 Forwarding and secondary distribution 12
8.3 Case 1: No forwarding 12
8.4 Case 2: Content not changed and EDIM responsibility forwarded 13
8.5 Case 3: EDIM responsibility not forwarded 15
9 EDI naming, addressing and use of directory 17
10 EDI security 17
11 Intercommunication with physical delivery services 18
11.1 Introduction 18
11.2 Delivery and notifications 18
11.3 Transfer of EDIM responsibility 18
11.4 Physical rendition 19
12 Use of message store for EDI 21
13 Elements of service 21
14 Classification of elements of service 21
14.1 Basic EDI messaging service 21
14.2 EDI messaging service optional user facilities 22

15 Quality of service....25
15.1 EDI message status....25
15.2 Support by providers of EDI service....25
15.3 Model of delivery and notification times....25
15.4 EDI message delivery time targets....26
15.5 EDI notification time targets....27
15.6 Error protection....27
15.7 Availability of service....27

ANNEXES

A– Glossary of terms....28
B – Definitions of elements of service....32
C – Security overview....37
D – EDI naming, addressing, and use of directory....45
E – Cross referencing overview....50

TABLES

1 – Case 1: No forwarding....13
2 – Case 2: EDIM responsibility forwarded....14
3 – Case 3: EDIM responsibility not forwarded....17
4 – Provision and use of secure messaging elements of service by MHS components....18
5 – Elements of service belonging to the basic EDI messaging service....21
6 – EDI messaging optional user facilities selectable on a per-message basis....23
7 – EDI messaging service optional user facilities agreed for a contractual period of time....25
8 – EDIN time targets....27

FIGURES

1 – EDI messaging environment....6
2 – EDI messaging system....7
3 – Information flow in EDI messaging system....8
4 – EDI messaging service functional mode....9
5 – EDI message structure....10
6 – EDI message structure for a typical EDI transaction....10
7 – Case 1: No forwarding....12
8 – Case 2: EDIM responsibility forwarded....14
9 – Case 3: EDIM responsibility not forwarded, Part 1....16
10 – Case 3: EDIM responsibility not forwarded....16
11 – M/PD delivery and notification times model....20
12 – Notification time model....26
C-1 – EDIM Responsibility transfer....42
D-1 – DIT structure for EDI requirements....46
D-2 – An aliasing example....47
D-3 – A country oriented aliasing example....48
E-1 – Cross referencing in EDI messaging....50

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 10021-8 was prepared by ITU-T (as ITU-T Recommendation F.435) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* in parallel with its approval by national bodies of ISO and IEC.

ISO/IEC 10021 consists of the following parts, under the general title *Information technology — Message Handling Systems (MHS)*:

- *Part 1: System and Service Overview*
- *Part 2: Overall Architecture*
- *Part 3: Abstract Service Definition Conventions*
- *Part 4: Message Transfer System: Abstract Service Definition and Procedures*
- *Part 5: Message Store: Abstract Service Definition*
- *Part 6: Protocol Specification*
- *Part 7: Interpersonal Messaging System*
- *Part 8: Electronic Data Interchange Messaging Service*
- *Part 9: Electronic Data Interchange Messaging System*

Annexes A and B form an integral part of this part of ISO/IEC 10021. Annexes C, D and E are for information only.

Introduction

This part of ISO/IEC 10021 is one of a number of parts of ISO/IEC 10021 (Information technology - Message Handling Systems (MHS)).

Message handling systems and services enables users to exchange of messages on a store-and-forward basis. A message submitted by one user (the *originator*) is conveyed by the Message Transfer System (MTS), the principal component of a larger Message Handling System (MHS), and is subsequently delivered to one or more other users, the message's *recipients*. A user may interact directly with the MTS, or indirectly via a message store (MS).

The MTS comprises a variety of interconnected functional entities called message transfer agents (MTAs). MTAs cooperate to transfer messages and deliver them to their intended recipients. Message stores (MSs) provide storage for messages and enable their submission, retrieval and management. User agents (UAs) help users access MHS. Access units (AUs) provide links to other communication systems and services of various kinds (e.g., other telematic services, postal services).

This part of ISO/IEC 10021 was initially developed and published by the ITU-T in 1991. The ITU-T version is published as CCITT Recommendation F.435 (1991) as amended by the MHS Implementor's Guide (version 12).

This part of ISO/IEC 10021 defines the overall system and service description of the message handling application called EDI Messaging.

ISO/IEC NOTE

As stated in the ITU-T version of this part of ISO/IEC 10021 [i.e., F.435 (1991)], the expression "Administration" is used for conciseness to indicate both a telecommunication Administration and a recognized private operating agency.

This page intentionally left blank

Information technology - Message Handling Systems (MHS) -

Part 8 :
Electronic Data Interchange Messaging Service

1 Scope

This part of ISO/IEC 10021 defines the overall system and service of EDI messaging.

Other aspects of message handling systems and services are defined in other parts of ISO/IEC 10021. The layout of Standards | Recommendations defining the message handling system and services is shown in table 1 of ISO/IEC 10021–1 | CCITT Recommendation X/F.400. The public services built on MHS, as well as access to and from the MHS for public services are defined in the ITU-T's F.400-Series of Recommendations.

The technical aspects of MHS are defined in the multi-part series numbered ISO/IEC 10021 and ITU-T's X.400-Series of Recommendations. The overall system architecture of MHS is defined in ISO/IEC 10021–2 | CCITT Recommendation X.402. The technical aspects of EDI messaging are defined in ISO/IEC 10021–9 | CCITT Recommendation X.435.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10021. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 10021 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 9594-2:1990, *Information technology – Open Systems Interconnection – The Directory – Part 2: Models.*
(See also CCITT Recommendation X.501 (1988))

ISO/IEC 9594-7:1990, *Information technology – Open Systems Interconnection – The Directory – Part 7: Selected object classes.*
(See also CCITT Recommendation X.521 (1988))

ISO/IEC 9594-8:1990, *Information technology – Open Systems Interconnection – The Directory – Part 8: Authentication framework.*
(See also CCITT Recommendation X.509 (1988))

ISO 9735:1988, *Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules.*

ISO/IEC 10021-1:1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS) - Part 1: System and Service Overview.*
(See also CCITT Recommendation F.400 (1992) | X.400 (1993))

ISO/IEC 10021-2:1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS) - Part 2: Overall Architecture.*
(See also CCITT Recommendation X.402 (1992))

ISO/IEC 10021-5:1994, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS) - Part 5: Message Store: Abstract Service Definition.*
(See also CCITT Recommendation X.413 (1992))

ISO/IEC 10021-7:1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS) - Part 7: Interpersonal Messaging System.*
(See also CCITT Recommendation X.420 (1992))

ISO/IEC 10021-9:1995, *Information technology – Message Handling Systems (MHS) - Part 9: Electronic Data Interchange Messaging System.*
(See also CCITT Recommendation X.435 (1991))

CCITT Recommendation F.401 (1992), *Message handling services: Naming and addressing for public message handling services.*

CCITT Recommendation F.415 (1992), *Message handling services: Intercommunication with public physical delivery services.*

3 Definitions

For the purposes of this part of ISO/IEC 10021, the following definitions, and those defined in annex A apply.

Definitions of the elements of service applicable to EDI messaging are contained in annex B of this part of ISO/IEC 10021. The elements of service applicable to the Message Transfer service, and used by EDI messaging, are called out in this part of ISO/IEC 10021, however their definitions are contained in ISO/IEC 10021-1 | CCITT Recommendation F.400, annex B.

3.1 Terms defined in this part of ISO/IEC 10021

3.1.1 EDI forwarding: Onward transfer of a received EDIM to one or more recipients determined by the forwarding EDI user agent/message store.

EDI forwarding takes place when an EDI message having been delivered to an EDI user agent or EDI message store is forwarded onward to another EDI user agent or EDI message store.

3.1.2 EDI message: Information in electronic form that is transferred between EDI messaging users. An EDI message is a member of the primary class of information objects conveyed between EDI messaging users.

See also ISO/IEC 10021-9 | CCITT Recommendation X.435 clause 8.

3.1.3 EDI messaging user: User that engages in EDI messaging. An EDI messaging user originates, receives, or both originates and receives EDI messages. The EDI messaging environment contains any number of EDI messaging users. An EDI messaging user may be a person or a computer process. An EDI messaging user may access the EDI messaging system through an access unit.

3.1.4 EDI notification: Member of the secondary class of information objects that indicates to the originator of an EDI message the disposition of EDIM responsibility for the EDI message.

3.1.5 EDI message responsibility: EDI message responsibility indicates whether the subject EDI message has been made available to a specific user by its EDI user agent/message store. EDI message responsibility carries no legal significance within this part of ISO/IEC 10021 and ISO/IEC 10021-9 | CCITT Recommendation X.435.

3.2 Terms imported from ISO 9735

- Acknowledgment request
- Application reference
- Communication agreement ID
- Date/time of preparation
- Functional group header
- Interchage control reference
- Interchange header
- Interchange recipient
- Interchange sender
- Message header
- Processing priority code
- Recipients reference, password
- Service string advice
- Syntax identifier
- Test indicator
- UNA
- UNB
- UNG
- UNH
- UNT
- UNZ

NOTE - These terms are further expanded in annex A of this part of ISO/IEC 10021 and annex K of ISO/IEC 10021-9 | CCITT Recommendation X.435.

3.3 Terms imported from ANSI X12

- Application reference
- Date and Time of Transmission
- GS
- Interchange header
- Functional group header
- Transaction set header
- ISA
- IEA
- Recipient;s transmission reference/password
- ST
- Transmission sender

- Transmission recipient
- Transmission priority code

NOTE - These terms are further expanded in annex A of this part of ISO/IEC 10021 and annex K of ISO/IEC 10021-9 | CCITT Recommendation X.435.

4 Abbreviations

ANSI	American National Standards Institute
AU	Access unit
DIT	Directory information tree
DL	Distribution list
DUA	Directory user agent
EDI	Electronic data interchange
EDIFACT	Electronic data interchange for Administration, commerce and transport
EDIM	EDI message
EDIME	EDI messaging environment
EDIMG	EDI messaging
EDIMS	EDI messaging system
EDI-AU	EDI access unit
EDI-MS	EDI message store
EDI-UA	EDI user agent
EDIN	EDI notification
FN	Forwarded notification
ID	Identifier
IPM	Interpersonal messaging
MD	Management domain
MH	Message handling
MHS	Message handling system
MS	Message store
MT	Message transfer
MTA	Message transfer agent
MTS	Message transfer system
NDN	Non-delivery notification
NN	Negative notification
O/R	Originator/Recipient
PD	Physical delivery
PDAU	Physical delivery access unit
PDS	Physical delivery system
PN	Positive notification
PRMD	Private management domain
TLMA	Telematic agent
UA	User agent
UNTDI	United Nations, trade data interchange
UTC	Coordinated universal time

5 Conventions

In clause 2, CCITT aligned standards are cited.

Common language practices have been applied as far as possible in the use of capitalization of words.

6 EDI messaging service

6.1 Introduction

The EDI messaging service provides an EDI messaging user with features to assist in communicating with other EDI messaging users. EDI messaging users are in many cases computer processes. The EDI messaging service uses the capabilities of the Message Transfer service (see also Recommendation F.410) for sending and receiving EDI messages. The elements of service describing the features of the EDI messaging service are defined in annex B, and classified in clause 14.

EDI, electronic data interchange, can be described as computer to computer exchange of structured business data, such as invoices and purchase orders. In some cases the EDI messaging service can be used to transmit an EDI interchange to a physical rendition system, such as a physical delivery system, or facsimile.

The EDI messaging service is provided by EDI messaging.

6.2 EDI messaging

EDI messaging (EDIMG) consists of the exchange of EDI messages (EDIMs), and EDI notifications (EDINs), which are information objects specified in ISO/IEC 10021-9 | CCITT Recommendation X.435.

6.3 EDI messaging environment

The environment in which EDI messaging takes place can be modelled as a functional object which is hereafter referred to as the EDI messaging environment (EDIME). When refined (i.e., functionally decomposed), the EDIME can be seen to comprise lesser objects referred to as the primary objects of EDI messaging. They include a single central object, the EDI messaging system (EDIMS), and numerous peripheral objects called EDI messaging users (EDIMG users).

The structure of the EDIME is depicted in figure 1.

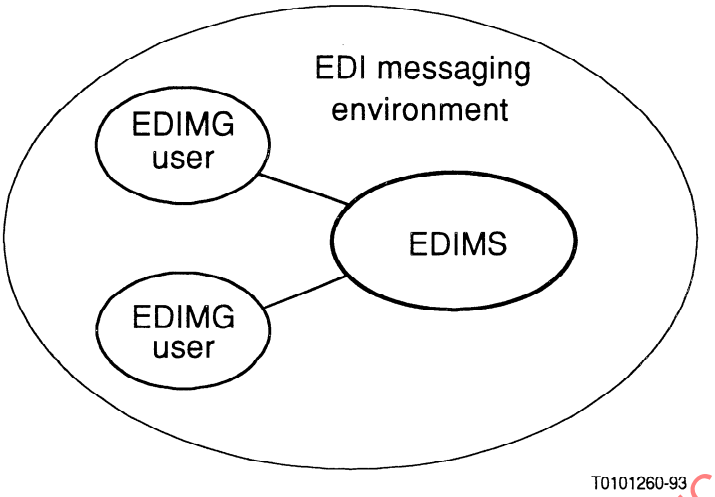


Figure 1 – EDI messaging environment

6.4 EDI messaging user

An EDI messaging user (EDIMG user) is a user that engages in EDI messaging. An EDIMG user originates, receives, or both originates and receives EDIMs. The EDIME contains any number of EDIMG users.

An EDIMG user may be a person or a computer process. An EDIMG user may access the EDIMS through an access unit.

7 EDI messaging system

7.1 Introduction

The EDI messaging system (EDIMS) is the functional object by means of which all EDIMG users communicate with one another in EDI messaging.

The EDIMS can be modelled as comprising lesser functional objects which interact with one another. These lesser objects are referred to as the secondary objects of EDI messaging. They include a single, central object, the message transfer system (MTS), and numerous peripheral objects of three kinds: EDI user agents (EDI-UAs), EDI message stores (EDI-MSs), and EDI access units (EDI-AUs).

The structure of the EDIMS is depicted in figure 2. As shown in figure 2, EDI-UAs, EDI-MSs, and EDI-AUs are the objects by which the EDIMS provides service to EDIMG users.

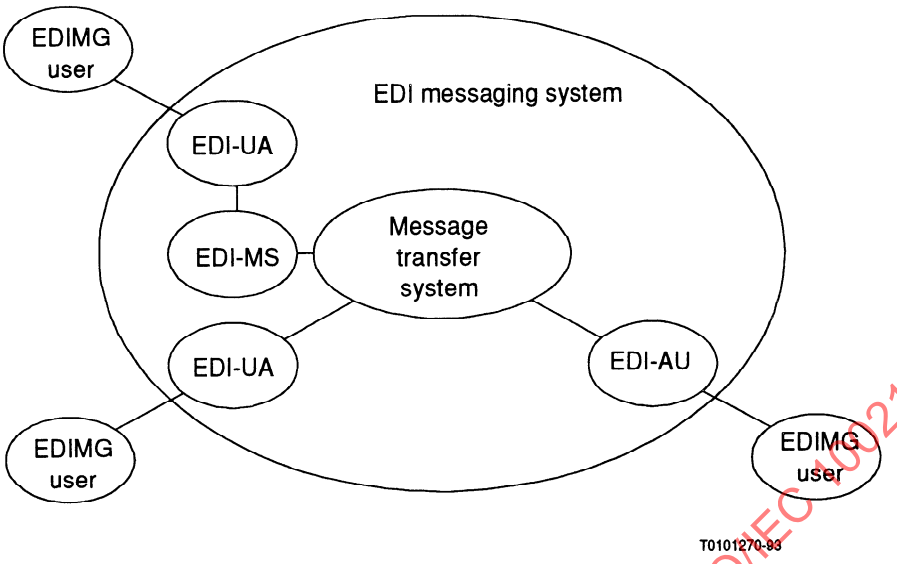


Figure 2 – EDI messaging system

7.1.1 EDI user agents

An EDI user agent (EDI-UA) is a user agent tailored so as to better assist a single EDIMG user to engage in EDI messaging. It helps that EDIMG user originate and receive messages containing EDIMs. The EDIMS contains any number of EDI-UAs.

NOTE – An exact definition of the boundary between the EDI-UA and the EDIMG user is beyond the scope of this part of ISO/IEC 10021.

7.1.2 EDI message store

An EDI message store (EDI-MS) is a message store tailored so as to better assist a single EDI-UA engage in EDI messaging. It helps that EDI-UA submit, take delivery of, store, and retrieve messages containing EDIMs.

7.1.3 Message transfer system

In the present context the message transfer system (MTS) conveys EDIMs or EDI notifications (EDINs) between EDI-UAs, or between an EDI-UA and an access unit. The EDIMS contains a single MTS.

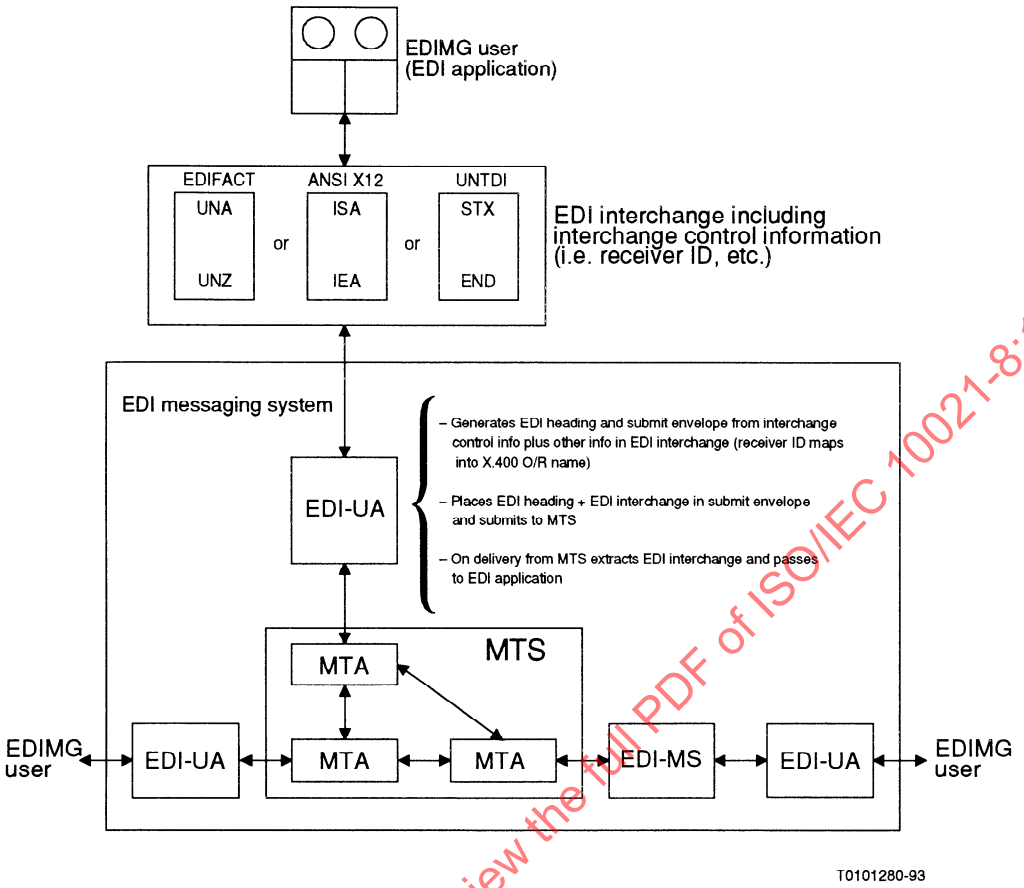
7.1.4 EDI access units

An EDIMG user may have access to/from the EDIMS through an access unit (AU). One type of access unit is the physical delivery access unit (PDAU). In EDIMG, the physical delivery access unit provides the ability to send messages to EDIMG recipients through a physical delivery system (PDS). Other types of EDI-AUs (e.g., facsimile access units) may be the subject of future standardization.

7.2 Information flow in the EDIMS

Figure 3 expands on figure 2 and shows the principal information flows in EDI messaging.

NOTE - Figure 3 illustrates aspects of the EDI encoded data exchanged in this model, not the actual details.



NOTES

1 - For abbreviations and acronyms see clause 4 and annex A of this part of ISO/IEC 10021.

2 - The structure of the information exchanged between the EDIMG user and the EDI-UA is not defined by this part of ISO/IEC 10021. In addition to the EDI interchange, the control information may comprise information carried in the envelope, EDIM heading, interchange header, etc. The control information could also be extracted from the EDI interchange and/or form other sources.

Figure 3 – Information flow in EDI messaging

7.3 EDI messaging service functional model

Figure 4 shows the functional model of the EDI messaging service. The UAs used in the EDI messaging service comprise a specific class of cooperating UAs. The optional PDAU allows EDIMG users to send messages to indirect users outside of the EDI messaging environment. The message stores used in the EDI messaging service have specific EDI related functions and can optionally be used by EDIMG users to take delivery of messages on their behalf. The telematic agent (TLMA) shown in figure 4 will allow access to telematic services and may be the subject of future standardization.

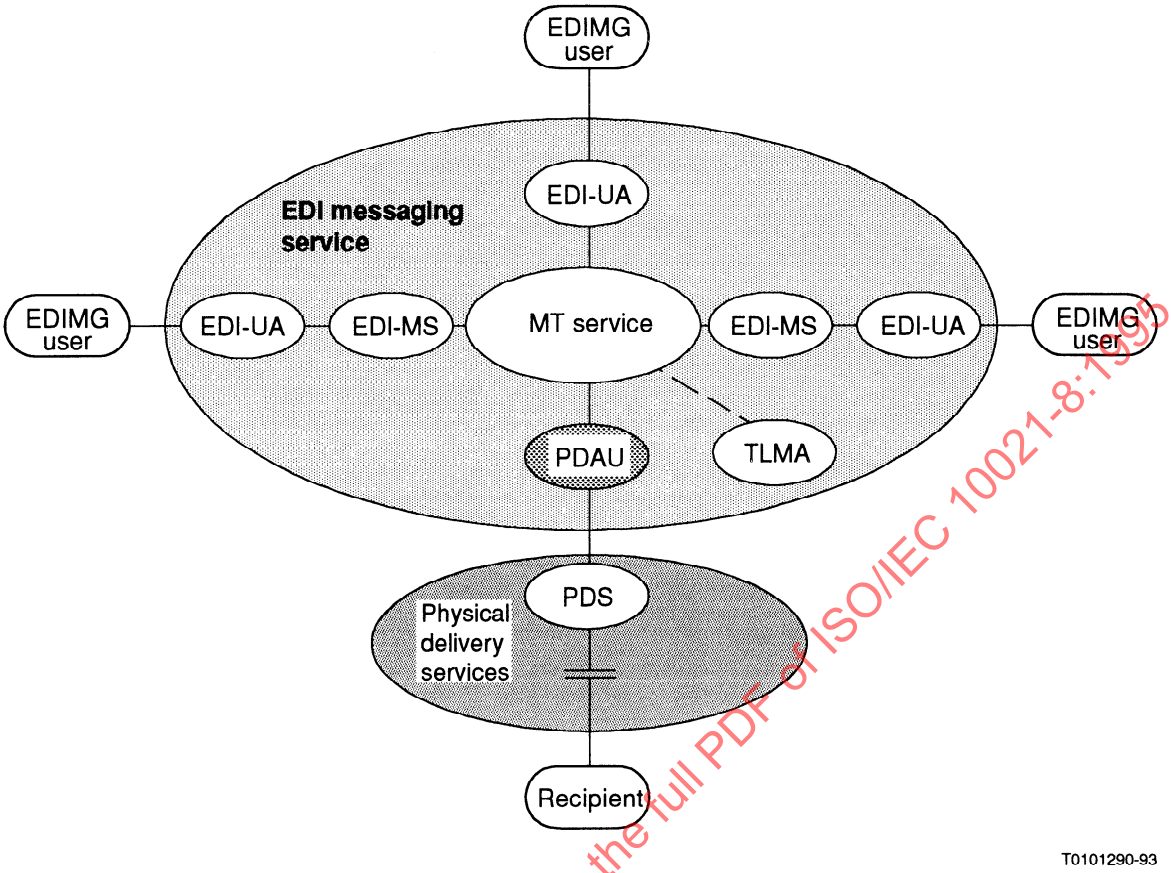


Figure 4 – EDI messaging service functional model

7.4 Structure of EDI messages

The EDI class of UAs create messages containing a content specific to the EDI messaging service. The specific content that is sent from one EDI-UA to another is a result of an originator, which is generally an application process, composing and sending a message, called an EDI message (EDIM). The EDIM carries the EDI interchange and optionally other information associated with the EDI interchange. Only one EDI interchange shall be present in an EDIM. Every EDIM shall contain an EDI interchange body part on origination of the EDIM. Any of the body parts can subsequently be removed (wholly, not partially) when forwarding an EDIM, except a forwarded body part, which cannot be removed. Body parts that are removed when forwarding are replaced with place holders to indicate what type of body part was removed. The heading of an EDIM shall not be removed when forwarding an EDIM. The structure of an EDIM as it relates to the basic message structure of MHS is shown in figure 5. The EDIM is conveyed with an envelope when being transferred through the MTS.

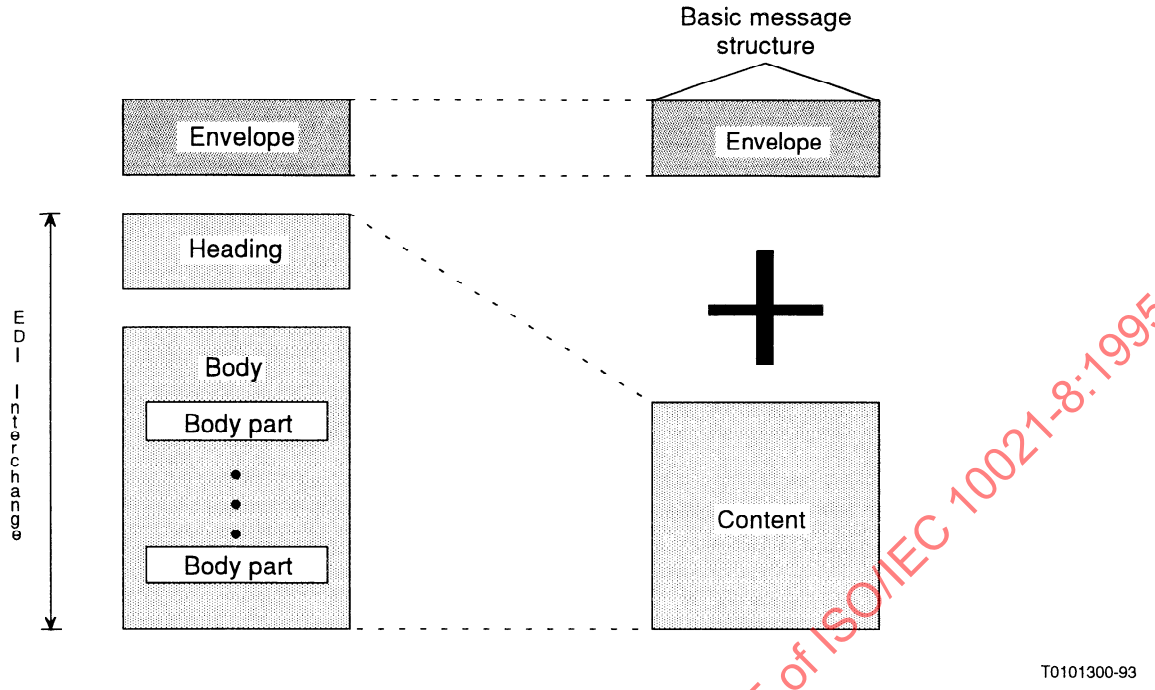


Figure 5 – EDI message structure

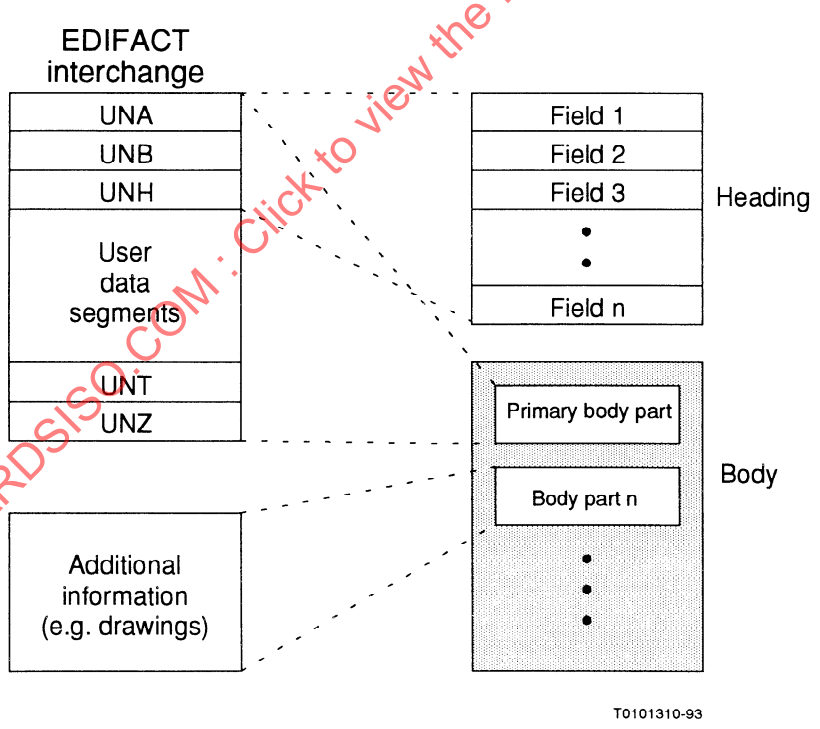


Figure 6 – EDI message structure for a typical EDI transaction

Figure 6 shows a mapping between a typical EDI interchange, and the corresponding EDI message structure. The EDI interchange is mapped entirely within one body part, called the primary body part, and may be an EDIFACT, ANSI X12, UNTDI or privately defined EDI interchange. Other body parts are available to convey information associated

with the EDI interchange such as drawings, explanatory text, etc. The heading of the EDIM contains various fields of information, some of which are present in the EDIFACT interchange header segments (or corresponding ISA or STX segments for ANSI X12 and UNTDI), and others containing service requests from the originator. The heading and body part(s) form the EDIM.

7.5 EDI notification

An EDIMG user can request that a recipient return an EDI notification (EDIN) indicating the disposition of the EDI message received. This notification is requested by an originating EDI-UA, and is generated by a recipient EDI-UA, EDI-MS, or AU. There are three possible conditions that can be requested and reported on, resulting in either the generation of a positive notification (PN), a negative notification (NN), or a forwarded notification (FN). The implied meanings of the responses PN, NN, and FN are described in 8.1. It is possible to forward a received EDI message unchanged and forward the obligation to respond to the notification request to the recipient to whom the EDI message is forwarded, or intermediate recipients, who then shall respond to the original originator of the message. An originating EDI-UA may request to be notified if the obligation to respond to the notification request has been forwarded. In this case, the EDI-UA or EDI-MS that forwards the EDIM shall send to the originating EDI-UA an EDI forwarded notification (FN).

In all cases, including notifications sent by EDI-UAs to whom the EDIM has been forwarded, the notifications shall contain the OR–name of the recipient that was specified by the original originator.

The originating EDI-UA may request any combination of the several EDINs from any combination of the recipients to whom the EDIM is sent. If no notifications are requested by an originator, none shall be sent by the recipient(s).

EDI notifications cannot be forwarded, and EDI notifications cannot be requested for EDINs.

8 EDIM responsibility and forwarding

8.1 Introduction

The EDIMS includes a concept called EDIM responsibility. This concept is key to the description below of EDINs and forwarding. In order to simplify the descriptions in the text below, all forwarding is shown as performed by the EDI-UA. It should be noted that the descriptions apply equally to forwarding performed by the EDI-MS.

The purpose for introducing the concept of EDIM responsibility is primarily to provide a method for confirming the passing of messages amongst EDI-UAs. EDIM responsibility may apply to access units in certain cases. The concept of EDIM responsibility is described as follows.

EDIM responsibility indicates that the EDIM is made available to the EDIMG user by the receiving EDI-UA. EDIM responsibility shall always be accepted when the EDI-UA adds or removes body parts when forwarding. An EDIM cannot leave the EDIMS unless EDIM responsibility has been accepted (delivery to a PDAU is a special case as described in 11.3). If requested to do so by the originating EDI-UA, the recipient EDI-UA, and possibly intermediate EDI-UAs (if requested), shall send EDINs to the originating EDI-UA.

When an EDI-UA receives an EDIM it shall, if requested to do so, inform the originating EDI-UA that the recipient EDI-UA has accepted or refused EDIM responsibility by sending an appropriate EDIN. Subclause 8.2 below contains a detailed description of the EDINs that are sent in various scenarios.

If notifications are requested, then when an EDI-UA accepts, refuses, or forwards EDIM responsibility, it shall send an appropriate EDIN to the originator, and if forwarding, it shall create the appropriate heading fields in the forwarded EDIM. The details of these operations are described in ISO/IEC 10021-9 | CCITT Recommendation X.435.

Body parts that are forwarded cannot be changed in any way. If EDIM responsibility is forwarded, the forwarded EDIM cannot be changed in any way. If EDIM responsibility is accepted, body parts may be removed from, or added to the original EDIM when creating the forwarded EDIM. Body parts that are removed when forwarding are replaced with place holders to indicate what type of body part was removed. EDIM responsibility forwarding is limited to only one recipient.

EDIMG includes mechanisms to prevent looping when forwarding.

8.2 Forwarding and secondary distribution

In EDIMG it may be desirable to receive EDI messages at a central EDI user agent, with subsequent forwarding to the final EDI user agents. Such a practice would, for example, enable a large organization to perform centralized functions such as logging, auditing, etc., on all EDI message traffic entering that organization. After performance of these functions the traffic would be distributed to the EDI user agents serving the recipient EDI applications. Similarly, a value added network service provider might operate a similar intermediary stage on behalf of its customers. The following text describes the use of an EDI-UA as such an intermediary stage.

Since an intermediate EDI-UA will generally not be the final EDI-UA, there is a need to provide end-to-end confirmation of EDIM responsibility acceptance for an EDIM within EDIMG. The element of service "EDI notification request" allows an originator to request from each recipient, positive, negative and forwarded notifications. Together with protocol elements defined in ISO/IEC 10021-9 | CCITT Recommendation X.435, the "EDI notification request" allows intermediate EDI-UAs to indicate, in a forwarded message, whether or not EDIM responsibility has been accepted. These tools allow EDIM responsibility acceptance to be deferred until an EDIM reaches the final EDI-UA, and provide an indication to that EDI-UA that a notification is to be returned to the original originator.

In order to illustrate the use of an EDI-UA as an intermediate stage, three cases are described below. In all cases, an EDIM originates in EDI-UA1 and terminates in EDI-UA3. EDI-UA2 is the intermediate EDI-UA. In cases 1 and 2 it is assumed that the EDIM is forwarded with content unchanged. In all three cases it is assumed that EDI-UA1 has requested notifications.

NOTE – Events described in the following tables are not necessarily performed in the exact sequential order shown in the tables.

8.3 Case 1: No forwarding

The EDIM prepared by EDI-UA1 is addressed to EDI-UA3. The EDIM is submitted to MTA1, transferred to MTA3, delivered to EDI-UA3 and retrieved by EDIMG user 3. EDI-UA3 will respond with an appropriate EDIN, accepting EDIM responsibility (i.e., PN). (If EDI-UA3 had determined that EDIMG user 3 could not retrieve the message, EDI-UA3 would have responded with an EDIN refusing EDIM responsibility (i.e., NN)). Figure 7 illustrates the flow of information. The sequence of EDIMs and EDINs is depicted in table 1.

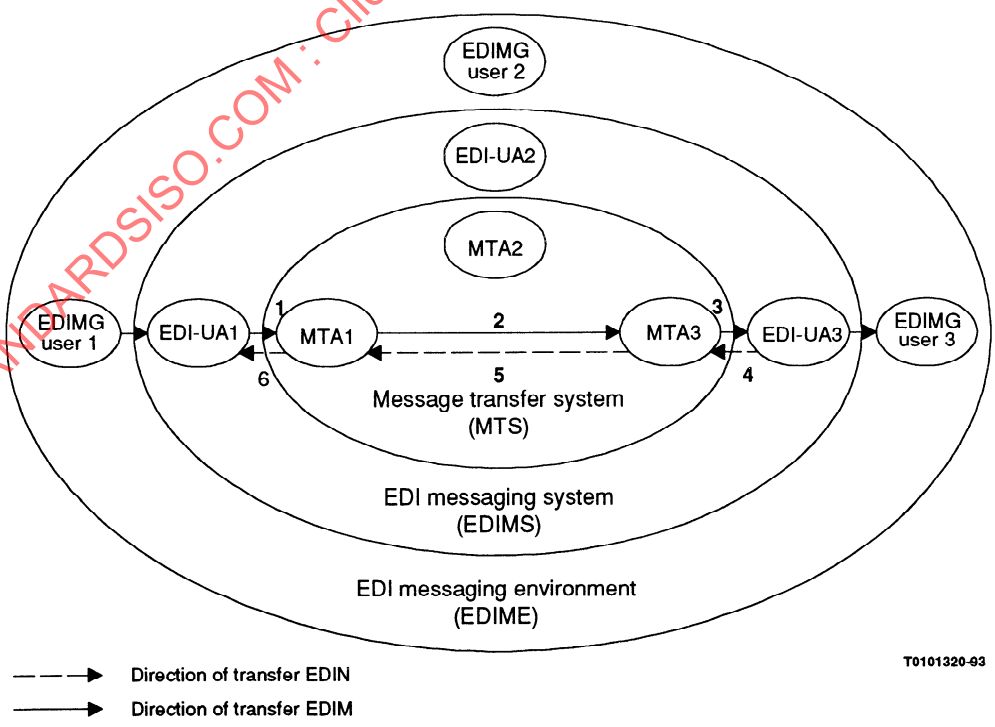


Figure 7 – Case 1: No forwarding

Table 1 – Case 1: No forwarding

Events	EDIM	EDIN
1	EDI-UA1 submits EDIM to MTA1	
2	MTA1 transfers EDIM to MTA3	
3	MTA3 delivers EDIM to EDI-UA3	
4		EDI-UA3 submits PN/NN to MTA3
5		MTA3 transfers PN/NN to MTA1
6		MTA1 delivers PN/NN to EDI-UA1

8.4 Case 2: Content not changed and EDIM responsibility forwarded

In this case an intermediary EDI-UA forwards a message from EDI-UA1 to EDI-UA3. The final recipient is EDI-UA3, and EDI-UA2 performs a forward operation, forwarding EDIM responsibility to EDI-UA3. The EDIM prepared by EDI-UA1 is addressed to EDI-UA2. The EDIM is delivered to EDI-UA2, which forwards it unchanged to EDI-UA3, based on selection criteria known to EDI-UA2.

EDIM responsibility is handled as follows:

When EDI-UA2 forwards EDIM responsibility, it shall create the forwarded EDIM so that requested EDINs are received by EDI-UA1, (see ISO/IEC 10021-9 | CCITT Recommendation X.435 for details). The following EDINs may be sent.

a) If EDI-UA1 requested notification of forwarding of EDIM responsibility, EDI-UA2 shall send forwarded notification - FN to EDI-UA1. This EDIN is sent when EDI-UA2 successfully submits the EDIM to MTA2.

b) If EDI-UA2 receives a non-delivery notification from MTA3 (via MTA2) it may send negative notification – NN to EDI-UA1.

NOTE - EDI-UA2 has the choice to send, or not to send, the EDIN in this case.

No other EDINs may be requested or sent. For example, EDI-UA2 cannot request notifications from EDI-UA3, and EDI-UA3 cannot send EDINs to EDI-UA2.

In the case of non-delivery, EDI-UA2 may attempt to resubmit the EDIM to the intended recipient. In this case, the NN to EDI-UA1 is sent only when EDI-UA2 determines that it shall no longer attempt to resubmit the EDIM to EDI-UA3.

c) If forwarding succeeds, EDI-UA3 shall send an appropriate EDIN to EDI-UA1, accepting or refusing EDIM responsibility.

Figure 8 illustrates the information flow described above for case 2. The sequence of possible EDIMs and EDINs is explained in table 2. Events (8, 11, 13, 15) and (10, 12, 14, 16) are mutually exclusive.

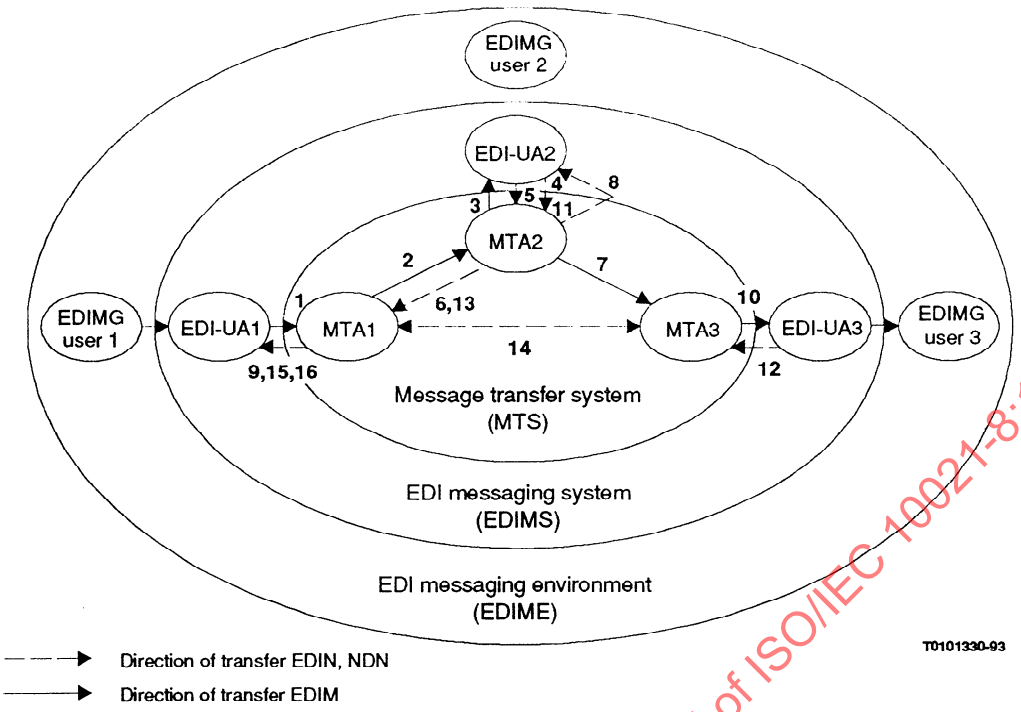


Figure 8 – Case 2: EDIM responsibility forwarded

Table 2 – Case 2: EDIM responsibility forwarded

Events	EDIM	EDIN	NDN
1	EDI-UA1 submits EDIM to MTA1		
2	MTA1 transfers EDIM to MTA2		
3	MTA2 delivers EDIM to EDI-UA2		
4		If requested, EDI-UA2 submits FN to MTA2	
5	EDI-UA2 submits forwarded EDIM to MTA2		
6		MTA2 transfers FN to MTA1	
7	MTA2 transfers EDIM to MTA3		
8			MTA2 sends NDN to EDI-UA2
9		MTA1 delivers FN to EDI-UA1	
10	MTA3 delivers EDIM to EDI-UA3		
11			EDI-UA2 submits NN to MTA2
12		EDI-UA3 submits PN/NN to MTA3	
13			MTA2 transfers NN to MTA1
14		MTA3 transfers PN/NN to MTA1	
15			MTA1 delivers NN to EDI-UA1
16		MTA1 delivers PN/NN to EDI-UA1	

The following should be noted:

1) EDI-UA1 will usually receive several EDINs if it requests FN (forwarded notification).
2) EDI-UA1 may receive EDINs in a sequence other than that in which they were created.
3) EDI-UA1 may receive no EDIN whatsoever even if it requested FN (for example, in the case of catastrophic failure of EDI-UA2 after MTA2 has delivered the EDIM to EDI-UA2).

It is up to EDI-UA1 to correctly handle 1 through 3 above. Item 1 can be handled for example, by keeping track of:

a) the EDIM ID,
b) the original recipient,
c) the submission time, and
d) the EDI notifications expected.

Item 2 can be handled by using the UTC time included in the EDIN (EDIN creation time). Item 3 can be handled with a time-out mechanism in EDI-UA1. Mechanisms to handle 1 to 3 are local implementation issues, thus beyond the scope of this part of ISO/IEC 10021.

8.5 Case 3: EDIM responsibility not forwarded

This scenario provides for the case where the EDIM prepared by EDI-UA1 is addressed to EDI-UA2, and EDI-UA2 accepts EDIM responsibility for the message prior to forwarding to EDI-UA3. This would occur, for example, if EDI-UA2 were to add or remove body parts when forwarding (changes of the content). When EDIM responsibility is accepted, EDI-UA2 sends an EDIN to the originator (i.e., PN), and creates the forwarded EDIM so that no further EDINs are received by EDI-UA1 (the originator) (see ISO/IEC 10021-9 \ CCITT Recommendation X.435 for details). As in case 2, EDI-UA1 addresses the EDIM to EDI-UA2. As in both previous cases EDI-UA3 represents the final destination.

Upon retrieval of the EDIM, EDI-UA2 returns an appropriate notification to EDI-UA1. The message is then forwarded to EDI-UA3. Since initial EDIM responsibility has now been accepted, EDI-UA2 is at liberty to request EDIM responsibility or not, as desired. If requested, the resulting EDIM responsibility relationship shall apply between EDI-UA3 and EDI-UA2, i.e. not end to end as in the previous cases. In the scenario described here EDIM responsibility is assumed to have been requested, with the result that EDI-UA3 responds to EDI-UA2 with an appropriate notification.

Figures 9 and 10 illustrate the flow of information for case 3. The sequence of EDIMs and EDINs for case 3 is explained in table 3.

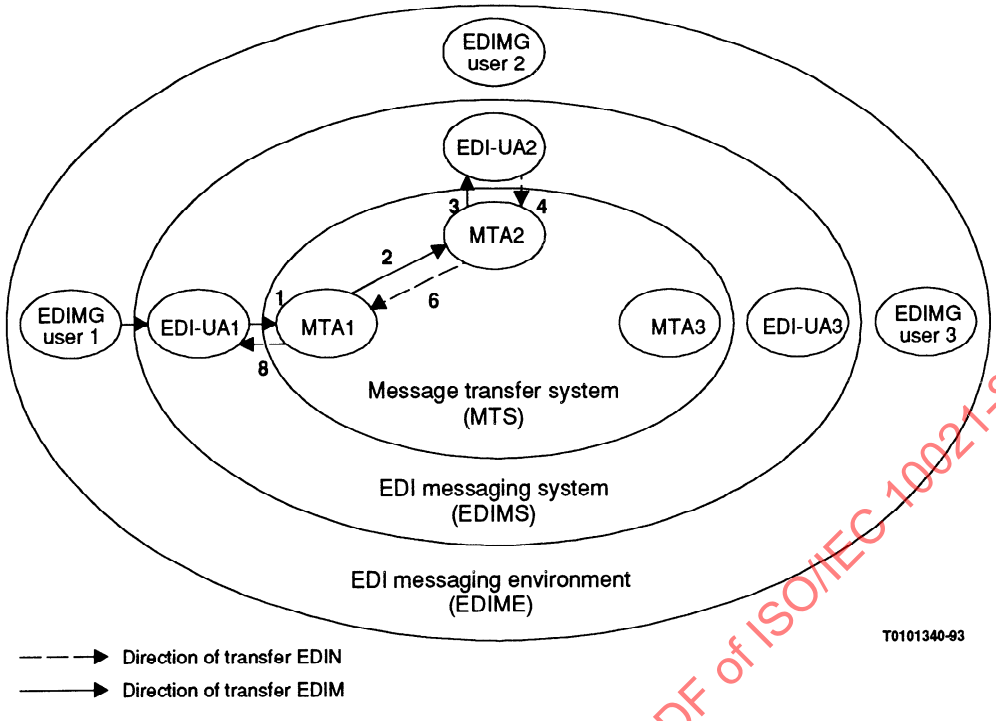


Figure 9 – Case 3: EDIM responsibility not forwarded, Part 1

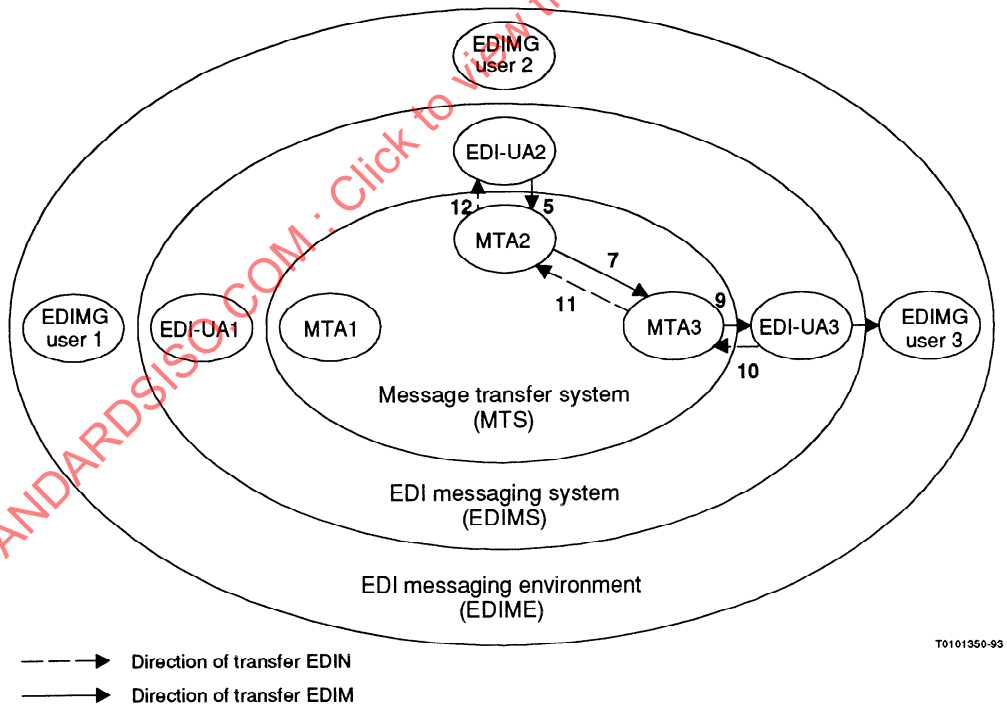


Figure 10 – Case 3: EDIM responsibility not forwarded, Part 2

Table 3 – Case 3: EDIM responsibility not forwarded

Events	Figure 9	Figure 10
1	EDI-UA1 submits EDIM to MTA1	
2	MTA1 transfers EDIM to MTA2	
3	MTA2 delivers EDIM to EDI-UA2	
4	EDI-UA2 submits PN to MTA2	
5		EDI-UA2 submits forwarded EDIM to MTA2
6	MTA2 transfers PN au MTA1	
7		MTA2 transfers EDIM to MTA3
8	MTA1 delivers PN to EDI-UA1	
9		MTA3 delivers EDIM to EDI-UA3
10		EDI-UA3 submits PN/NN to MTA3
11		MTA3 transfers PN/NN to MTA2
12		MTA2 delivers PN/NN to EDI-UA2

9 EDI naming, addressing and use of directory

The MHS use of Directory as defined in ISO/IEC 10021-1 | CCITT Recommendation X/F.400, clause 13 is used to provide the Directory services required for EDI messaging.

Each management domain should provide directory services for its EDIMG users.

EDI messaging, naming and addressing and the subsequent directory service requirements are outlined in annex D of this part of ISO/IEC 10021.

10 EDI security

The MHS security capabilities are defined in ISO/IEC 10021-1 | CCITT Recommendation X/F.400 in clause 15, and are also applicable for EDI messaging. In addition, the following extensions are provided to 15.4 of the above referenced document.

An overview of the extended security capabilities in EDIMG is as follows:

Proof of EDI notification: Enables the recipient of an EDIM to create an EDIN which may be used by the recipient of the EDIN to authenticate the originator of the EDIN.

Non-repudiation of the EDI notification: Provides the recipient of an EDIN with proof of the origin of the EDIN which will protect against any attempt by the originator of the EDIN from falsely denying sending the EDIN.

Proof of content received: Enables the originator of an EDIM to verify that the message content received by the recipient was the same as the message content originated by the originator.

Non-repudiation of content originated: Provides the recipient of the EDIM with proof that the message content received was the same as the message content originated. This protects against any attempt by the originator to falsely deny originating the message content.

Non-repudiation of content received: Provides the originator of the EDIM with proof that the message content received was the same as the message content originated. This proof will protect against any attempt by the recipient to falsely deny the content of the EDIM received.

Table 4 – Provision and use of secure messaging elements of service by MHS components

Elements of service	EDIM originator	MTS	EDIM recipient
Proof of EDI notification	U	-	P
Non-repudiation of EDI notification	U	-	P
Proof of content received	U	-	P
Non-repudiation of content originated	P	-	U
Non-repudiation of content received	U	-	P

P A provider of the service
U A user of the service

Annex C describes the EDIMS vulnerabilities and details how they are countered. Annex I of ISO/IEC 10021-9 | CCITT Recommendation X.435 supplements ISO/IEC 10021-2's | CCITT Recommendation X.402's MHS security model for EDIMS with EDI security features. ISO/IEC 10021-9 | CCITT Recommendation X.435 describes operations and procedures for security services.

11 Intercommunication with physical delivery services

11.1 Introduction

As defined in CCITT Recommendation F.415, MH/PD intercommunication is a generic capability of the Message Transfer service. To make use of this capability, the originator may use a postal O/R address on submission, or, if using a directory name on submission, select physical delivery as the "Requested delivery method" and choose any desired options from the MH/PD elements of service (table 1 of CCITT Recommendation F.415).

The originator provides the address of the recipient as defined in CCITT Recommendation F.401, postal O/R address. This may be done through the Directory.

11.2 Delivery and notifications

Delivery to the access unit occurs when the EDIM is passed from the final MTA to the PDAU (MTS to EDI-AU).

Delivery notifications and EDI notifications relevant to physical delivery apply as defined in CCITT Recommendation F.415 with the addition of an EDIN, as depicted below in figure 11.

These notifications are generated by the MTA/PDAU system components, which are considered to be co-located.

Definitions of "T" times are provided in CCITT Recommendation F.415; "$\mathbf{T_{edi}}$" can be defined as:

T_{edi} = Generation and delivery of the EDIN.

NOTES

1 – Start time corresponds to the time at which the EDIN is generated.

2 – End time corresponds to the time that the EDIN is made available to the EDIMG user.

11.3 Transfer of EDIM responsibility

While it is up to the PDAU to physically render and subsequently deliver an EDIM sent to it, a PDAU can never accept EDIM responsibility for an EDIM. If an "EDI notification request" is asked for, two possibilities exist for the PDAU. If it determines that it can render the EDIM for physical delivery, it shall return an FN to the originator of the EDIM. However, if it determines that it cannot render or deliver the EDIM, it shall return an NN to the originator of the EDIM.

11.4 Physical rendition

The basic physical rendition details defined in CCITT Recommendation F.415, annex B, should be used as a base, primarily for the rendition of routing and delivery information such as the address blocks, position on the page relative to the window, etc.

For hard copy physical rendition specific to EDI, three approaches are identified;

1) Standardized rendition
2) Privately defined rendition
3) Accompanying information for rendition (may be the subject of future standardization).

Alternatively, if rendition rules are not available, the EDIM could simply be printed "as is", if possible, assuming that the recipient is able to work with the information, possibly with guidelines provided through some other means or message. (Additional guidelines and rules for the physical rendition of EDIMs may be the subject of future standardization.)

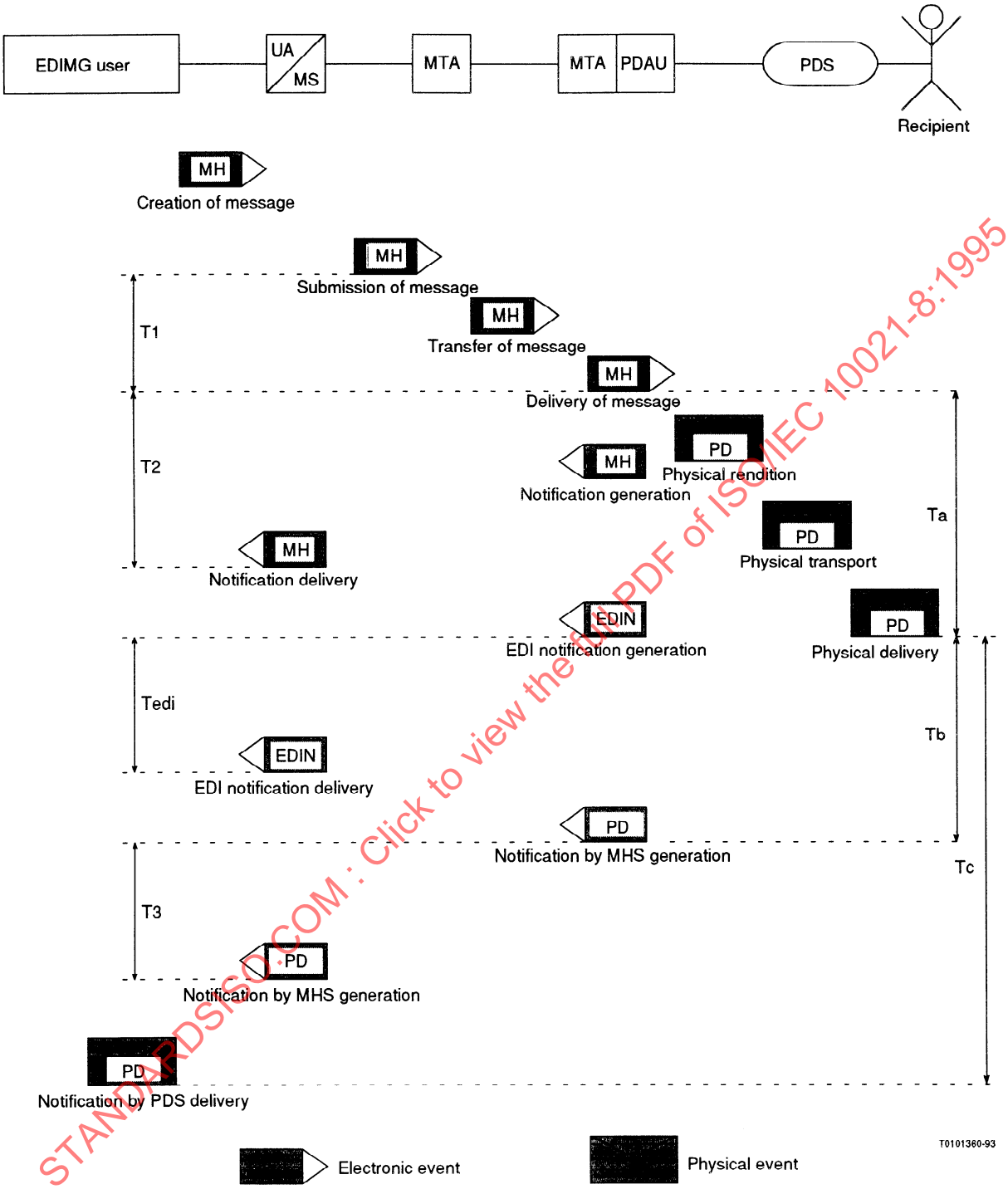


Figure 11 – M/PD delivery and notification times model

12 Use of message store for EDI

Message store features may be used for EDI messaging. The general MS elements of service, "stored message fetching", "stored message listing", "stored message summary", "stored message deletion", and "stored message alert" are applicable for EDI messaging.

General MS attributes and auto-actions are described in ISO/IEC 10021-5 | CCITT Recommendation X.413. EDI specific MS attributes and auto actions are described in ISO/IEC 10021-9 | CCITT Recommendation X.435.

An EDI specific MS element of service, "Stored EDI message auto-forward", provides suitable MS auto-forwarding capabilities for EDI messaging.

Security policies may restrict the use of message store elements of service.

13 Elements of service

Elements of service are particular features, functions, or capabilities of MHS. The elements of service applicable for EDI messaging are made up of MT elements of service and EDI messaging elements of service. The MT elements of service used in EDI messaging are called out in this part of ISO/IEC 10021 in tables 5 to 7, however they are defined in ISO/IEC 10021-1 | CCITT Recommendation F.400, annex B. The definitions of elements of service specific to EDI messaging are also listed in tables 5 to 7, and are defined in annex B. The realization of all the elements of service applicable to EDI messaging is described in other parts of this part of ISO/IEC 10021.

14 Classification of elements of service

14.1 Basic EDI messaging service

The basic EDI messaging service, which makes use of the MT service, enables an EDIMG user to send and receive EDI messages. An EDIMG user prepares EDI messages with the assistance of an EDI user agent (EDI-UA). EDI-UAs cooperate with each other to facilitate communication between their respective EDIMG users. To send an EDI message, the originating EDIMG user submits the message to his EDI-UA specifying the OR-name of the recipient who is to receive the EDI message. The EDI message, which has an identifier conveyed with it, is then sent by the originator's EDI-UA to the recipient's EDI-UA/MS via the Message Transfer service.

Following a successful delivery to the recipient's EDI-UA/MS, the EDI message is available for the recipient. To facilitate meaningful communication, a recipient can specify the encoded information type(s) contained in EDI messages that he will allow to be delivered to his EDI-UA, as well as the maximum length of an EDI message that he is willing to accept. The original encoded information type(s) and an indication if any conversions that have been performed and the resulting encoded information type(s) are supplied with each delivered EDI message. In addition, the submission time and delivery time are supplied with each EDI message. Non-delivery notification is provided with the basic MT service. The elements of service belonging to the basic EDI messaging service are listed in table 5.

Table 5 – Elements of service belonging to the basic EDI messaging service

Elements of service	References
Access management	B.1
Content type indication	B.12
Converted indication	B.15
Delivery time stamp indication	B.22
EDI message identification	EDI.8
Message identification	B.41
Non-delivery notification	B.47
Orginal encoded information types indication	B.54
Submission time stamp indication	B.89
Typed body	EDI.30
User/UA capabilities registration	B.93

NOTE – **B.** references are to annex B of ISO/IEC 10021-1 | CCITT Recommendation **X**/F.400, and EDI references are to annex B in this part of ISO/IEC 10021.

14.2 EDI messaging service optional user facilities

A set of the elements of service of the EDI messaging service are optional user facilities. The optional user facilities of the EDI messaging service, which may be selected on a per-message basis or for an agreed contractual period of time, are listed in table 6 and table 7, respectively.

The optional user facilities of the EDI messaging service that are selected on a per-message basis are classified for both origination and reception by EDI-UAs. If a management domain offers these optional user facilities for origination by EDI-UAs, then an EDIMG user is able to create and send EDI messages according to the procedures defined for the associated element of service. If a management domain offers these optional user facilities for reception by EDI-UAs/MSs/AUs, then the receiving EDI-UA/MS/AU shall be able to receive and recognize the indication associated with the corresponding element of service and to inform the EDIMG user of the requested optional user facility. Each optional user facility is classified as *additional* (A) or *essential* (E) for EDI-UAs/MSs/AUs from these two perspectives.

Table 6 – EDI messaging optional user facilities selectable on a per-message basis

Elements of service	Origination	Reception	References
Additional physical rendition	A	A	B.2
Alternate recipient allowed	E	E	B.3
Application security element	A	A	EDI.1
Basic physical rendition	A	E*	B.7
Character set	E	E	EDI.2
Content confidentiality	A	A	B.10
Content integrity	A	A	B.11
Conversion prohibition	E	E	B.13
Conversion prohibition in case of loss of information	A	A	B.14
Counter collection	A	E*	B.16
Counter collection with advice	A	A	B.17
Cross reference information	A	E	EDI.3
Deferred delivery	E	N/A	B.19
Deferred delivery cancellation	E	N/A	B.20
Delivery notification	E	N/A	B.21
Delivery via bureaufax service	A	A	B.23
Designation of recipient by directory name	A	N/A	B.24
Disclosure of other recipients	E	E	B.25
DL expansion history indication	N/A	E	B.26
DL expansion prohibited	A	N/A	B.27
EDI forwarding	A	N/A	EDI.4
EDI message type(s)	E	E	EDI.5
EDI notification request	E	E	EDI.6
EDI standard indication	E	E	EDI.7
EDIM responsibility forwarding allowed indication	E	E	EDI.9
EDIN receiver	A	E	EDI.10
EMS (Express Mail Service)[a)]	A	E*	B.28
Expiry date time indication	A	E	EDI.11
Explicit conversion	A	N/A	B.30
Grade of delivery selection	E	E	B.32
Incomplete copy indication	A	E	EDI.12
Interchange header	E	E	EDI.13
Latest delivery designation	A	N/A	B.39
Message flow confidentiality	A	N/A	B.40
Message origin authentication	A	A	B.42
Message security labelling	A	A	B.43
Message sequence integrity	A	A	B.44
Multi-destination delivery	E	N/A	B.45
Multi-part body	A	E	EDI.14
Non-repudiation of content originated	A	A	EDI.15
Non-repudiation of content received	A	A	EDI.16
Non-repudiation of content received request	A	A	EDI.17
Non-repudiation of delivery	A	A	B.49
Non-repudiation of EDI notification	A	A	EDI.18
Non-repudiation of EDI notification request	A	A	EDI.19
Non-repudiation of origin	A	A	B.50
Non-repudiation of submission	A	A	B.51
Obsoleting indication	A	E	EDI.20
Ordinary mail	A	E*	B.53
Originator indication	E	E	EDI.21
Originator requested alternate recipient	A	N/A	B.56

Table 6 *(concluded)*

Elements of service	Origination	Reception	References
Physical delivery notification by MHS	A	A	B.57
Physical delivery notification by PDS	A	E*	B.58
Physical forwarding allowed	A	E*	B.59
Physical forwarding prohibited	A	E*	B.60
Prevention of non-delivery notification	A	N/A	B.61
Probe	A	N/A	B.63
Probe origin authentication	A	N/A	B.64
Proof of content received	A	A	EDI.22
Proof of content received request	A	A	EDI.23
Proof of delivery	A	A	B.65
Proof of EDI notification	A	A	EDI.24
Proof of EDI notification request	A	A	EDI.25
Proof of submission	A	N/A	B.66
Recipient indication	E	E	EDI.26
Redirection disallowed by originator	A	N/A	B.68
Registered mail	A	A	B.70
Registered mail to addressee in person	A	A	B.71
Related message(s)	A	E	EDI.27
Report origin authentication	A	A	B.74
Request for forwarding address	A	A	B.75
Requested preferred delivery method	A	A	B.76
Services indication	A	A	EDI.28
Special delivery[a)]	A	E*	B.81
Stored message deletion	N/A	E***	B.84
Stored message fetching	N/A	E***	B.85
Stored message listing	N/A	E**	B.86
Stored message summary	N/A	E**	B.87
Undeliverable mail with return of physical message	A	E*	B.91
Use of distribution list	A	N/A	B.92

E Essential optional user facility shall be provided

E* Essential optional user facility only applying to PDAUs

E** Essential optional user facility only applying to MSs

E*** Essential optional user facility applying to MSs and UAs

A Additional optional user facility may be provided

N/A Not applicable

a) At least EMS or "Special delivery" shall be supported by the PDAU and associated PDS.

NOTES

1 – Bilateral agreement may be necessary in cases of reception by EDI-UA of elements of service classified as "A".

2 – **B.** references are to annex B of ISO/IEC 10021-1 | CCITT Recommendation X/F.400, and EDI references are to annex B of this part of ISO/IEC 10021.

Table 7 – EDI messaging service optional user facilities agreed for a contractual period of time

Elements of service	Classification	References
Alternate recipient assignment	A	B.4
Hold for delivery	A	B.33
Implicit conversion	A	B.34
MS register	A	B.nn[a)]
Redirection of incoming messages	A	B.69
Restricted delivery	A	B.77
Secure access management	A	B.79
Stored EDI message auto-forward	A	EDI.29
Stored message alert	A	B.82
Stored message auto-forward	A	B.83[b)]

a) This element of service shall be defined and assigned a "B" number in the next publication of ISO/IEC 10021-1 | CCITT Recommendation X/F.400. It describes a capability that is supported in ISO/IEC 10021-5 | CCITT Recommendation X.413, but not described in ISO/IEC 10021-1 | CCITT Recommendation X/F.400.

b) The use of this element of service, which is a general MS capability, is discouraged for EDI messaging. "Stored EDI message auto-forward", which is an EDI specific MS capability, provides a suitable alternative.

NOTE – **B.** references are to annex B of ISO/IEC 10021-1 | CCITT Recommendation X/F.400, and EDI references are to annex B of this part of ISO/IEC 10021.

15 Quality of service

15.1 EDI message status

The unique identification of each EDI message enables the system to provide information about e.g., the status of an EDI message.

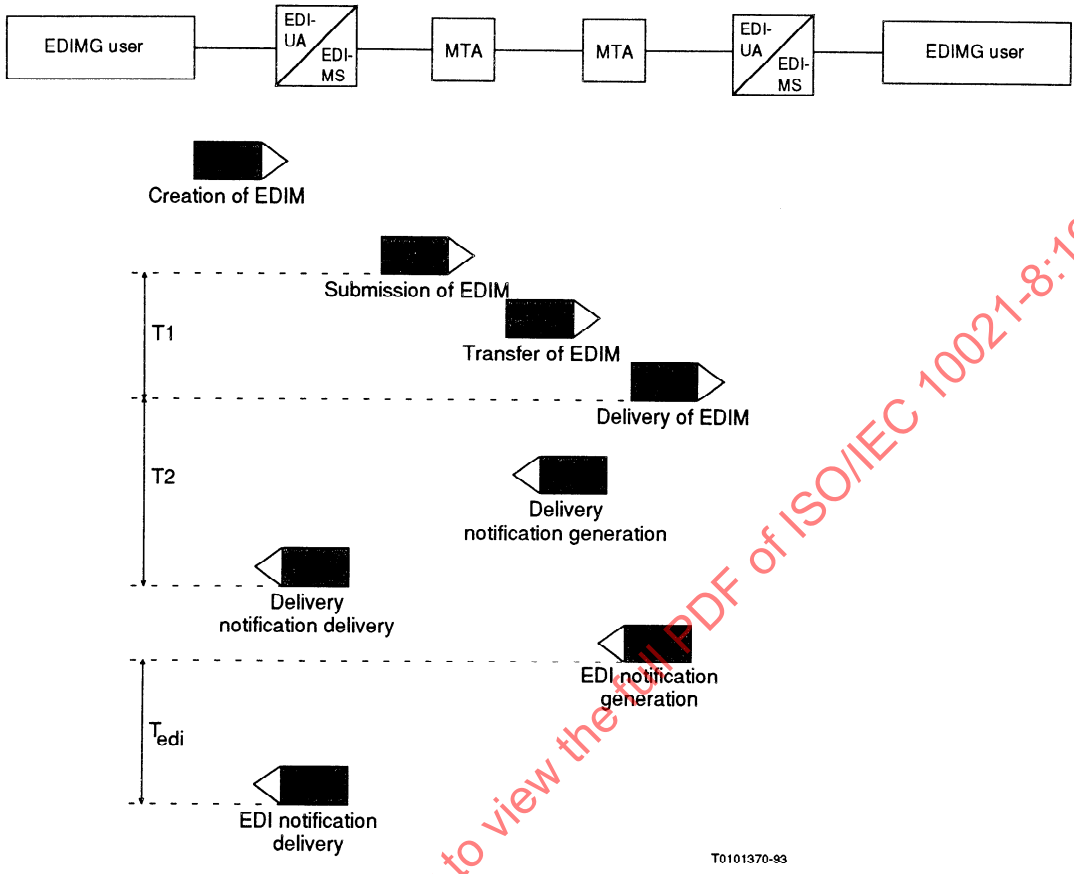
In the event of system failure all accepted and non-delivered EDI messages should be traceable. If EDI messages cannot be delivered, the originator shall be informed by a "Non-delivery notification" unless the originator invoked "Prevention of non-delivery notification".

15.2 Support by providers of EDI service

Service providers should provide assistance to their subscribers, with regard to non-delivery notifications not being received in due time, as far as system components are concerned. Additional provision of support for status and tracing of messages may be provided under national responsibility.

15.3 Model of delivery and notification times

See figure 12.



T1 Delivery time

Note 1– Start time of T1 corresponds to the submission time stamp indication.
Note 2– End time of T1 corresponds to the delivery time stamp indication.

T2 Delivery notification

Note 1– Start time of T2 corresponds to the delivery time stamp indication.
Note 2– End time of T2 is the time the delivery notification is made available to the EDIMG user through the EDI-UA or EDI-MS.

T_{edi} Generation and delivery of EDI notification

Note 1– Start time corresponds to the time at which the EDIN is generated.
Note 2– End time corresponds to the time that the EDIN is made available to the EDIMG user.

Figure 12 – Notification time model

15.4 EDI message delivery time targets

The delivery time targets (including transfer times) are dependent on the message transfer system, on the number of transiting domains, and on message sizes. Values significantly less than those currently specified for the IPM service are aimed at.

The management domain of the recipient EDI-UA should force non-delivery notification if the EDI message has not been delivered within *x* hours after submission (or after date and time indicated for deferred delivery), the value of *x* being dependent on the grade of delivery requested by the originator.

The specification of these values for the EDI service may be the subject of future standardization.

15.5 EDI notification time targets

Delivery time targets for EDI notifications depend on local arrangements. When EDINs are initiated by the receiving EDI-UA they have the same time targets as the EDI messages that caused them to occur (see table 8).

Table 8 – EDIN time targets

Grade of delivery	95% delivered before
Urgent	15 minutes
Normal	60 minutes
Non-urgent	4 hours

NOTES
1 – Intercommunication with PRMDs is not included in the calculation of the time targets.

2 – The values are provisional and due for revision after proven experience.

3 – For quality of service for physical delivery see clause 11.

4 – Achieving these time targets relies heavily on the MTS timings.

15.6 Error protection

Error protection on transmission is provided by the MHS and underlying protocols used in the provision of the EDI service.

15.7 Availability of service

In principle the EDI service should be available continuously. The EDI-UA or the EDI-MS should be available for submission or delivery continuously (unless hold for delivery is invoked). In cases where the EDI-UA is not available for delivery continuously, an EDI-MS should be used.

Annex A
(normative)

Glossary of terms

NOTE – The explanations given below are not necessarily definitions in the strict sense. See also the definitions in annex B and the Glossary in ISO/IEC 10021-1 | CCITT Recommendation X/F.400 and terms provided in the other parts of ISO/IEC 10021 (especially ISO/IEC 10021-9 | CCITT Recommendation X.435). The terms have, depending on the source, varying levels of abstraction.

A.1 EDI application

A computer process that creates and/or processes EDI messages.

See also clause A.13.

A.2 EDI interchange

"Communication between partners in the form of a structured set of messages and service segments starting with an interchange control header and ending with an interchange control trailer" (see ISO 9735).

In the context of EDI messaging, the contents of the primary body part of an EDI message.

A.3 **EDI message** (EDIM)

See definition in clause 3.

A.4 EDI message store (EDI-MS)

See definition in ISO/IEC 10021-9 | CCITT Recommendation X.435, in subclause 3.5.

A.5 **EDI messaging** (EDIMG)

EDI messaging consists of the exchange and associated procedures of EDI messages and EDI notifications, which are information objects specified in ISO/IEC 10021-9 | CCITT Recommendation X.435.

A.6 **EDI messaging environment** (EDIME)

The environment in which EDI messaging takes place can be modelled as a functional object which is referred to as the EDI messaging environment. When refined (i.e., functionally decomposed), the EDIME can be seen to be comprised of lesser objects referred to as the primary objects of EDI messaging. They include a single central object, the EDI messaging system, and numerous peripheral objects called EDI messaging users.

A.7 EDI messaging service

A service that provides an EDI messaging user with features to assist in communicating with other EDI messaging users. EDI messaging users are in many cases computer processes. The EDI messaging service uses the capabilities of the message transfer service for sending and receiving EDI messages. Certain elements of service describing the features of the EDI messaging service are defined in annex B, and classified in clause 14.

A.8 **EDI messaging system** (EDIMS)

The EDI messaging system is the functional object by means of which users communicate with one another in EDI messaging.

The EDI messaging system can be modelled as comprising lesser functional objects which interact with one another. These lesser objects are referred to as the secondary objects of EDI messaging. They include a single, central object, the message transfer system, and numerous peripheral objects of three kinds: EDI user agents, EDI message stores, and EDI access units.

A.9 **EDI messaging user** (EDIMG user)

See definition in 3.3 of this part of ISO/IEC 10021.

NOTE – In the context of ISO/IEC 10021-9 | CCITT Recommendation X.435, for conciseness the term "user" is used with the meaning "EDIMG user".

See also clause A.13 below.

A.10 **EDI notification** (EDIN)

See definition in 3.4.

In EDI messaging an EDIMG user can request that a recipient return an EDI notification indicating the disposition of the EDI message it received. This notification is requested by an originating EDI user agent, and is generated by a recipient EDI user agent/message store, or access unit. There are 3 possible conditions that can be requested and reported on, resulting in either the generation of a positive notification (PN), a negative notification (NN), or a forwarded notification (FN). The one notification serves to carry either the positive notification, the negative notification, or the forwarding notification. It is possible to forward a received EDI message unchanged and forward the obligation to respond to the notification request to the forwarded recipient, or intermediate recipients, who then shall respond to the original originator of the message. An originating UA may request to be notified if the obligation to respond to the notification request has been forwarded. In this case, the UA or MS that forwards the EDI message will send to the originating UA an EDI forwarded notification.

In all cases, including notifications sent by UAs to whom the EDI message has been forwarded, the notifications shall contain the O/R name of the recipient that was specified by the original originator.

The originating UA may request any combination of the several EDI notifications from any combination of the recipients to whom the EDI message is sent. If no notifications are requested by an originator, none shall be sent by the recipient(s).

EDI notifications cannot be forwarded, and EDI notifications cannot be requested for EDI notifications.

A.11 **EDI message responsibility**

See definition in 3.5.

NOTE – EDIM responsibility is a trace-keeping means for confirming and tracking the passage of EDI messages among EDI user agents and EDI message stores.

A.12 **EDI security**

The MHS security capabilities as defined in ISO/IEC 10021-1 | CCITT Recommendation X/F.400, in clause 15 and ISO/IEC 10021-2 | CCITT Recommendation X.402, in clause 10, are used for EDI to provide the security features for the EDI messaging system. EDI messaging system vulnerabilities and how they are countered are outlined in annex C of this part of ISO/IEC 10021.

A.13 **EDI user**

See ISO/IEC 10021-9 | CCITT Recommendation X.435.

The EDI user is an object not necessarily belonging to the EDI messaging environment. In the context of message handling, largely identical with an EDI messaging user.

See also clauses A.1 and A.9 above, and the NOTE to clause A.14.

A.14 **EDI user agent** (EDI-UA)

See definition in ISO/IEC 10021-9 | CCITT Recommendation X.435.

NOTE – An exact definition of the boundary between the EDI-UA and the EDI messaging user is beyond the scope of this part of ISO/IEC 10021.

A.15 Electronic data interchange (EDI)

EDI can be defined as computer to computer exchange of structured business data, such as invoices and purchase orders. In the context of the MHS multi part series, it refers to the standardized way of performing the interchange by using the protocol means of ISO/IEC 10021-9 | CCITT Recommendation X.435, and the service outlined in this part of ISO/IEC 10021.

A.16 GS

Functional group header.

Segment name in ANSI X12.

A.17 IEA

Interchange trailer.

Segment name in ANSI X12.

A.18 Interchange

See EDI interchange in A.2.

A.19 ISA

Interchange header.

Segment name in ANSI X12.

A.20 MHD

Message header.

Segment name in UNTDI.

A.21 ST

Transaction set header.

Segment name in ANSI X12.

A.22 STX

Start of transmission.

Defined in UNTDI.

A.23 UNA

Service string advice.

Defined in EDIFACT.

A.24 UNB

Interchange header.

Segment name in EDIFACT.

A.25 UNG

Functional group header.

Segment name in EDIFACT.

A.26 UNH

Message header.

Segment name in EDIFACT.

A.27 UNT

Message trailer.

Segment name in EDIFACT.

A.28 UNZ

Interchange trailer.

Segment name in EDIFACT.

Annex B
(normative)

Definitions of elements of service

This annex contains definitions for the elements of service unique to EDI messaging. It does not contain definitions for those elements of service of the MT service applicable to EDI messaging. Those are contained in ISO/IEC 10021-1 | CCITT Recommendation X/F.400, annex B. The abbreviation *PR* in the title line means that this element of service is available to be used on a per-recipient basis.The numbering for EDI elements of service uses, for ease of reference, and to distinguish them from message transfer and IPM elements of service, the abbreviation "**[EDI.n]**".

B.1 application security element [EDI.1]

Element of service that allows the originator and the recipient to indicate in the heading of the EDI message application security information in order to support end-to-end security services.

B.2 character set [EDI.2]

Element of service that allows the originator to indicate in the heading of an EDI message, the character set used in the EDI body of the message.

B.3 cross reference information [EDI.3]

Element of service that allows the originator to indicate in the heading of an EDI message, information that can be used for cross referencing between application specified reference IDs within an EDI interchange and body parts of this or other EDI messages.

B.4 EDI forwarding [EDI.4]

Element of service that enables an EDI-UA to forward with or without changes, and an EDI-MS to forward without changes, a received EDIM. Support of the element of service "EDIN receiver" is also required when forwarding.

B.5 EDI message type(s) [EDI.5]

Element of service that allows the originator to indicate in the heading of an EDI message the type(s) of EDI messages contained in the EDI interchange (e.g., invoices, purchase orders, etc.).

B.6 EDI notification request [EDI.6] PR

Element of service that allows the originating EDI-UA to request that it be notified of a recipient's acceptance, refusal or forwarding of EDIM responsibility, in any combination, for the message carrying this request. The originating EDI-UA conveys this request to the recipient EDI-UA/MS/AU.

If the recipient EDI-UA/MS accepts EDIM responsibility for the message it issues a positive notification (PN) back to the originator of the message and no further notifications are issued back to this originator for this message.

In the case where the recipient EDI-UA/MS does not accept EDIM responsibility and successfully forwards the message with content unchanged, the forwarded recipient UA/MS, or optionally any intermediate UAs/MSs, has the same obligations as the first recipient UA/MS with respect to responding to this request, and the response is due to the original originator of the message. A forwarding notification (FN) is sent back to the originator.

If the recipient EDI-UA/MS/AU refuses EDIM responsibility for the message, or is unable to successfully forward the message, it issues a negative notification (NN) back to the originator of the message, with a reason indicated. Reasons for refusing EDIM responsibility for the message are as follows:

1) the EDI interchange could not be passed over to the EDIMG user;

2) the EDI interchange could not be passed over to the EDIMG user within a specified time limit;
3) the message was discarded before processing;
4) the recipient's subscription was terminated after delivery but before responding;
5) EDI forwarding and forwarding of EDIM responsibility was attempted, but failed;
6) PDAU could not render the message;
7) security error;
8) unspecified local reasons;

In the case of physical delivery access units, a PN is not meaningful, so a forwarded notification (FN) is returned to the originator instead of a PN.

A negative notification indicates that this message shall not be made available to the EDIMG user and implies that the EDIM shall not be processed by an EDI application.

Subject to the security policy, the capabilities of the message store may be restricted, e.g., when a secure notification is requested, the message store shall not be allowed to generate a PN.

B.7 EDI standard indication [EDI.7]

Element of service that enables the originating EDI-UA to indicate in the heading of an EDI message the type of EDI standard that is being used in this EDI message (e.g., EDIFACT, etc).

B.8 EDI message identification [EDI.8]

Element of service that enables cooperating EDI-UAs to convey a globally unique identifier for each EDI message sent or received. The EDI message identifier is composed of an OR-name of the originator and an identifier that is unique with respect to that name. EDI-UAs and EDIMG users use this identifier to refer to a previously sent or received EDI message (for example, in EDI notifications).

B.9 EDIM responsibility forwarding allowed indication [EDI.9] PR

Element of service that allows an originating EDI-UA to indicate that the EDIM responsibility for this EDI message may be forwarded on by the recipient EDI-UA.

B.10 EDIN receiver [EDI.10]

Element of service that allows the originator, or a forwarding EDI-UA/MS, to indicate to a recipient the O/R address that requested notifications should be returned to.

B.11 expiry date/time indication [EDI.11]

Element of service that allows the originator to indicate to the recipient the date and time after which the originator considers the EDI message to be invalid. The intent of this element of service is to state the originator's assessment of the current applicability of an EDI message. The particular action by the recipient, or by the recipient's EDI-UA, is unspecified. Possible actions might be to file or delete the EDI message after the expiry date has passed.

B.12 incomplete copy indication [EDI.12]

Element of service that allows a forwarding EDI-UA to indicate that the forwarded EDI message is an incomplete copy of an EDI message with the same EDI message identification in that one or more body parts of the original EDI message are absent.

B.13 interchange header [EDI.13]

Element of service that enables the originating EDI-UA to place data elements of the EDI interchange headers in corresponding fields in the EDIM.

B.14 multi-part body [EDI.14]

Element of service that allows an originator to send to a recipient an EDI message with a body that is comprised of several parts. The nature and attributes, or type, of each body part are conveyed along with the body part.

B.15 non-repudiation of content originated [EDI.15]

Element of service that enables an originating EDI-UA to provide a recipient EDI-UA with an irrevocable proof as to the authenticity and integrity of the content of the message as it was submitted into the MH environment.

The corresponding proof data can be supplied in two ways depending on the security policy in force:

1) Using the Non-repudiation of Origin security service applied to the original message or,
2) By means of a notarization mechanism.

NOTE – Use of a notarization mechanism is not reflected in protocol elements, but is subject to bilateral agreement.

B.16 non-repudiation of content received [EDI.16] PR

Element of service that enables an originating EDI-UA to get from a recipient EDI-UA an irrevocable proof that the original subject message content was received by the recipient EDI-UA and EDIM responsibility was accepted, forwarded or refused. This service provides irrevocable proof as to the integrity of the content received and irrevocable proof as to the authenticity of the recipient of the message. It will protect against any attempt by the recipient(s) to subsequently deny having received the message content. This service is stronger than the "Proof of Content Received" service.

The corresponding proof data can be supplied in two ways depending on the security policy in force:

1) By returning a "non-repudiation of origin" of the "EDI notification" which incorporates the following:
   - the originator's "non-repudiation of origin" arguments (if present),
   - the complete original message content, if the originator's "non-repudiation of origin" arguments are not present.
2) By means of a notarization mechanism.

NOTE – Use of a notarization mechanism is not reflected in protocol elements, but is subject to bilateral agreement.

B.17 non-repudiation of content received request [EDI.17] PR

Element of service that enables the originating EDI-UA to request the recipient EDI-UA to provide it with an irrevocable proof of the received message content by means of an EDI notification.

NOTE – This element of service requires the "EDI notification request" also to be present.

B.18 non-repudiation of EDI notification [EDI.18] PR

Element of service that provides the originator of a message with irrevocable proof that the subject message was received by the recipient EDI-UA and EDIM responsibility was accepted, forwarded or refused.

This shall protect against any attempt by the recipient EDI-UA to deny subsequently that the message was received and that the EDIM responsibility for the message has been accepted as indicated. This element of service provides the originator with irrevocable proof of the "proof of EDI notification".

Such a proof may be provided by means of the "Non-repudiation of Origin" security service, currently defined in ISO/IEC 10021-2 | CCITT Recommendation X.402 in § 10.2.5.1, applied to the notification.

This service is stronger than the "Proof of EDI Notification" service.

B.19 non-repudiation of EDI notification request [EDI.19] PR

Element of service, used in conjunction with "EDI notification request", that enables the originating EDI-UA to request the responding EDI-UA to provide it with irrevocable proof of the origin of the notification.

NOTE – This element of service supersedes the "Proof of EDI notification request" and assumes that "EDI Notification Request" is already present.

B.20 obsoleting indication [EDI.20]

Element of service that allows the originator to indicate to the recipient that one or more EDI messages previously sent by the originator are obsolete. The EDI message that carries this indication supersedes the obsolete EDI message(s).

The action to be taken by the recipient or the recipient's EDI-UA is a local matter. The intent, however, is to allow the EDI-UA or the recipient to, for example, remove or file an obsolete message(s).

B.21 originator indication [EDI.21]

Element of service that allows the identity of the originator to be conveyed to the recipient.

B.22 proof of content received [EDI.22] PR

Element of service that allows an originating EDI-UA to get from a recipient EDI-UA proof that the original subject message content was received by the recipient EDI-UA and EDIM responsibility was accepted, forwarded or refused.

The corresponding proof is obtained by returning a proof of origin of the EDI notification which incorporates the originator's message origin authentication and/or content integrity arguments, if present, or the complete original message content otherwise.

B.23 proof of content received request [EDI.23] PR

Element of service that enables the originating EDI-UA to request the recipient EDI-UA to provide it with proof of the received message content by means of an EDI notification.

NOTE – This element of service requires the "EDI notification request" to also be present.

B.24 proof of EDI notification [EDI.24] PR

Element of service that allows the originator of a message to obtain the means to corroborate that the subject message was received by the recipient EDI-UA and EDIM responsibility was accepted, forwarded or refused. Such a corroboration is provided by means of the MTS user-to-MTS user "Message Origin Authentication" security service, currently defined in ISO/IEC 10021-2 | CCITT Recommendation X.402, subclause 10.2.1.1.1, applied to the EDI notification.

B.25 proof of EDI notification request [EDI.25] PR

Element of service, used in conjunction with "EDI notification request", that enables the originating EDI-UA to request the responding EDI-UA to provide it with a corroboration of the source of the EDI notification.

NOTE – This element of service assumes that "EDI notification request" is already present.

B.26 recipient indication [EDI.26] PR

Element of service that allows the originator to provide the names of one or more EDIMG users, or DLs, who are intended recipients of the EDI message. In addition it is possible to specify an action request qualifier for each recipient, such as;

1) for action;
2) copy;
3) other, as defined bilaterally.

NOTE – The qualifier represents intent on the part of the originator with respect to the EDIM, however the recipient is not necessarily bound by this intent.

B.27 related message(s) [EDI.27]

Element of service that allows the originator to associate with the EDI message being sent, the globally unique identifiers of one or more other messages which share the same identification space (e.g., IP-messages), see ISO/IEC 10021-7 | CCITT Recommendation X.420. This enables the recipient's EDI-UA, for example, to retrieve from storage a copy of the referenced messages.

B.28 services indication [EDI.28]

Element of service that allows the originator to indicate in the heading of the EDI message various service requests to service suppliers that have bilateral meaning outside this part of ISO/IEC 10021.

B.29 stored EDI message auto-forward [EDI.29]

Element of service that allows a user of an EDI-MS to have the message store automatically perform EDI forwarding, with or without accepting EDIM responsibility. The user of the EDI-MS may establish criteria for selecting EDIMs through use of the element of service "MS register". The complete EDIM, as received from the originator, is forwarded unchanged, and if requested, an appropriate EDIN is generated by the EDI-MS. EDIM responsibility forwarding is limited to only one recipient. Support of the element of service "EDIN receiver" is also required when forwarding.

Subject to the requirements of the security policy in force, the capabilities of the message store may be restricted, e.g., when a secure notification is requested, the message store shall not be allowed to generate a PN.

B.30 typed body [EDI.30]

Element of service that permits the nature and characteristics of the body of an EDI message to be conveyed along with the body. Permissible body part types are EDI body, forwarded EDIM body, and externally defined body parts.

Annex C
(informative)

Security overview

C.1 Introduction

This annex details the vulnerabilities identified within an EDIME and the resulting security services required to counter those vulnerabilities.

This annex is based on the assumption that an EDIME may use the secure messaging services as defined in ISO/IEC 10021-1 | CCITT Recommendation X/F.400. However, where vulnerabilities are not adequately covered by the existing MHS security services, provision has been made in ISO/IEC 10021-9 | CCITT Recommendation X.435 for additional security services in the EDIME.

Some of the security services defined for the EDIME are of a generic message handling nature, others are specific to the EDIME. The security services defined for the EDIME are specific to EDIMG and are therefore fully defined in ISO/IEC 10021-9 | CCITT Recommendation X.435.

C.2 Vulnerabilities

In most of the areas identified below, there will also be further vulnerabilities and corresponding service considerations at the level of the EDI applications (i.e., EDIMG users). The security model reflected in this paper assumes that such considerations are outside the scope of this part of ISO/IEC 10021. The EDIMG security model assumes that the EDIMG user provides adequate security and trusted functionality in the operation of EDI applications sufficient to meet the user's security policy.

NOTE – In practice this may necessitate co-location of the EDI application and the EDI-UA unless a suitably secure environment is established which includes both components.

The following description of vulnerabilities is based on the threat definitions in annex D of ISO/IEC 10021-2 | CCITT Recommendation X.402. In addition, it has been considered necessary to examine message loss independently of message sequencing and modification of information, and to take account of further vulnerabilities for EDIMG which are not currently identified in ISO/IEC 10021-2 | CCITT Recommendation X.402.

An important aspect of the EDI environment which is not recognised within the ISO/IEC 10021-2 | CCITT Recommendation X.402 security model is the concept of EDIM responsibility for messages at each stage of the message path through the MHS environment.

In an EDI context, the increased possibility of a number of service providers offering commercial services may require that the forwarding of EDIM responsibility be clearly identified and assured to provide further protection, not only to end users but also to such service providers.

It is therefore necessary to establish the concept of EDIM responsibility domains, which may involve additional consideration of legal issues. One possible division of the EDIME into EDIM responsibility domains is as follows:

- EDIMG user environment plus the EDI-UA;
- MTS management domain;
- EDI message store (if not co-located with either of the above).

C.2.1 Masquerade

As defined in ISO/IEC 10021-2 | CCITT Recommendation X.402, annex D.

C.2.2 Message sequencing

As defined in ISO/IEC 10021-2 | CCITT Recommendation X.402, annex D.

Users should not assume that EDIMs shall be delivered in correct sequence. EDI applications should be able to recover from duplication and out-of-sequence messages, provided that MHS offers protection against the modification of information while messages are within the MHS environment.

C.2.3 Message loss

Vulnerability to message loss is considered critical in the EDIMG environment.

Two types of message loss are distinguished:

- catastrophic failure of an EDI-UA, EDI-MS or MTA,
- loss of individual message(s).

EDI messaging users and service providers may need to consider more carefully issues concerning transfer of messages between EDIM responsibility domains:

- from the originating EDI-UA user domain;
- between relaying domains;
- to the recipient EDI-UA user domain.

C.2.4 Modification of information

As defined in ISO/IEC 10021-2 | CCITT Recommendation X.402, annex D.

C.2.5 Denial of service

As defined in ISO/IEC 10021-2 | CCITT Recommendation X.402, annex D.

C.2.6 Repudiation

As defined in ISO/IEC 10021-2 | CCITT Recommendation X.402, annex D.

Furthermore repudiation vulnerability in the EDIM environment is considered to be critical. Such vulnerability may be increased by use of certain MHS services (e.g., auto-forwarding, redirection).

C.2.7 Leakage of information

As defined in ISO/IEC 10021-2 | CCITT Recommendation X.402, annex D.

C.2.8 Manipulation of information by EDIMG user

The EDI community has additionally identified a further vulnerability where the integrity of a message content is altered subsequent to EDI interchange (i.e., by either or both of the originating EDI-UA and recipient EDI-UA). This vulnerability includes manipulation of message content in the originator's local store after non-repudiation of submission and/or manipulation of message content in the recipient's store after non-repudiation of delivery.

C.2.9 Other vulnerabilities

Other vulnerabilities are considered important such as:

- misrouting;
- misdelivery (especially important in the context of redirection);
- insider threats;
- receipt of data that the EDI application is not prepared to accept.

NOTE - The vulnerability of *misrouting* is expanded in ISO/IEC 10021-2 | CCITT Recommendation X.402.

C.3 Vulnerabilities countered

ISO/IEC 10021-2 | CCITT Recommendation X.402, clause 10 provides an abstract security model for Message Transfer. The security model provides a framework for describing security services that counter potential vulnerabilities within the MTS and between MTS-User to MTS-User. EDIMG vulnerabilities may also be countered

by security services which are outside the existing model in ISO/IEC 10021-2 | CCITT Recommendation X.402. The following text describes how the EDIM vulnerabilities are countered using ISO/IEC 10021-2 | CCITT Recommendation X.402 security services, enhanced security services defined in ISO/IEC 10021-9 | CCITT Recommendation X.435 and pervasive mechanisms defined in this part of ISO/IEC 10021.

C.3.1 Masquerade

The existing MHS security services which counter this vulnerability are:

- message origin authentication;
- secure access management;
- security labelling;
- proof of delivery;
- proof of submission.

Since an EDI-UA/MS is deemed in the MHS architecture as belonging to one user, it is not considered appropriate to provide selective access control for the various operations that may be performed on a EDI-MS. However, there is a requirement for security audit trail to record the actions of the EDIMG user.

In this part of ISO/IEC 10021 such security audit trails are expected to be implemented as pervasive mechanisms (the term pervasive mechanism is defined in ISO/IEC 7498-2). Protocols to support audit capability may be the subject of future standardization.

C.3.2 Message sequencing

The existing MHS Security service which counters this vulnerability is:

- message sequence integrity.

This security service has limited effect as it is based on the provision of an integer by the originating EDI-UA with no assurance as to uniqueness or consecutiveness.

It is considered that the MHS environment should not be required to ensure message sequence integrity, but should support detection of sequence integrity failure (by additional provision of audit/logging facilities and/or the provision of third party notary services). In this part of ISO/IEC 10021 it is considered the responsibility of the EDIMG user to recover from sequence errors and message duplication.

C.3.3 Message loss

Message loss could occur potentially over any peer-to-peer communications link (e.g., by deliberate malicious act), or by the failure or incorrect behaviour (whether by malicious intent or otherwise) of any MHS component (EDI-UA, EDI-MS, MTA). The following categories of message loss are distinguished:

- catastrophic message loss (i.e. failure of a component);
- loss of individual messages in the EDI-MS – whether malicious or accidental;
- MTS message loss.

C.3.3.1 Catastrophic failure

Failure of the EDI-UA is outside the scope of this part of ISO/IEC 10021.

Failure of the EDI-MS is potentially catastrophic and desirably needs some protection, at least in terms of detection. This should be provided by an offline archive to hold all submitted and delivered messages. In this part of ISO/IEC 10021 detection and recovery from message loss using such archive mechanisms is a local matter.

Failure of any component in the MTS may similarly be catastrophic and can again be protected by offline archive of messages. As for the message store, detection and recovery from message loss using such archive mechanisms in the MTS is a local matter, and outside the scope of this part of ISO/IEC 10021.

C.3.3.2 EDI-MS specific message loss

Loss of individual messages in the message store – whether malicious or accidental – shall require the provision of a secure audit trail to enable detection of such loss. Such a service may need to be provided to the EDIMG user and to EDI-MS management. In this part of ISO/IEC 10021, secure EDI-MS audit trail could be realized as a pervasive mechanism and is a local issue. Protocol to support an audit trail may be the subject of future standardization.

C.3.3.3 MTS specific message loss

Loss of individual messages in the MTS (whether malicious or accidental) shall also require the provision of a secure audit trail to enable detection of such loss. Such a mechanism would need to be provided on a per-MTA and a per-MD basis depending on security policy in force. A secure MTA/MTS audit trail could be realized as a pervasive mechanism and is a local issue. The protocol to support an audit trail may be the subject of future standardization.

C.3.3.4 End-to-end message loss

The following description assumes that the functionality of the EDI-UA (including any associated components to meet such functionality – e.g., encryption devices) is trusted.

The existing "Message Sequence Integrity" service does not guarantee detection of message loss, since it relies on the provision of an integer value by the originating EDI-UA. In practice, effective operation of this service may be achieved with a common code of practice between EDIMG users which is outside the scope of this part of ISO/IEC 10021.

As a result, MHS services which may provide an indication of message loss are confined to services offered to the originating EDIMG user. Whereas, the existing "Proof of Submission and Delivery" services provide some degree of confidence that the message has not been lost they do not operate end-to-end. In particular they do not take account of the scenario where the recipient EDI-UA and EDI-MS are not co-located. There is therefore a requirement for a Proof of Receipt (i.e., by the recipient EDI-UA) service. This capability is realized by the user requesting an EDI notification which may be secured. The EDI notification indicating the status of EDIM responsibility as accepted, forwarded or refused includes elements which associates the notification with the subject message.

In an EDIMG environment proof of receipt may therefore be provided by signing the EDI Notification service using the existing MTS security elements. In particular the EDI-UA to EDI-UA security service of "message origin authentication" may be used to *sign* the EDI notification on submission of the EDI notification to the MTS. In this part of ISO/IEC 10021 the requirement for proof of receipt may be implemented by a trusted form of EDI notification in the EDIMG environment.

NOTE – This service is called "proof of EDI notification" and/or "non-repudiation of EDI notification" in EDIMG depending on the strength of the mechanism provided.

The MTS mechanism used on message submission to provide this service is defined as the MTS submission abstract operation in ISO/IEC 10021-4 / CCITT Recommendation X.411, subclause 8.2.1.1.1.28 "Content-integrity-check". In this instance the message content is the EDI notification. Proof of association between the subject message and replying EDI notification is provided by subject message EDI identifier and if included in the subject message the message content-integrity-check argument.

C.3.4 Modification of information

The existing MHS security services which counter this vulnerability are:

- connection integrity;
- content integrity.

These security services provide sufficient protection against modification of message content. It is also noted that use of double enveloping (i.e., with encrypted checksum on outer envelope) may provide additional protection.

NOTE – EDI-UAs are trusted entities in terms of content integrity.

C.3.5 Denial of service

This is a very important vulnerability for EDIMG users, but is outside the scope of this part of ISO/IEC 10021.

C.3.6 Repudiation

Services which offer protection against repudiation in the EDIMG environment are fundamentally concerned with formalizing the forwarding of EDIM responsibility.

The security services as defined in ISO/IEC 10021-2 | CCITT Recommendation X.402 are:

- non-repudiation of origin;
- non-repudiation of submission ;
- non-repudiation of delivery.

These security services only cover some areas of transfer between EDIM responsibility domains, which may be of significance in an EDIMG environment (as illustrated in figure C-1). Areas which are not covered by security services provided in 1992 for message handling include:

- between EDIMG user domains (i.e., end-to-end);
- between MTS management domains;
- between an EDI message store and a recipient EDI-UA.

Therefore services and/or pervasive mechanisms defined in this part of ISO/IEC 10021 cover the above deficiencies:

- non-repudiation/proof of transfer;
- non-repudiation/proof of retrieval;
- non-repudiation/proof of edi notification;
- non-repudiation/proof of content.

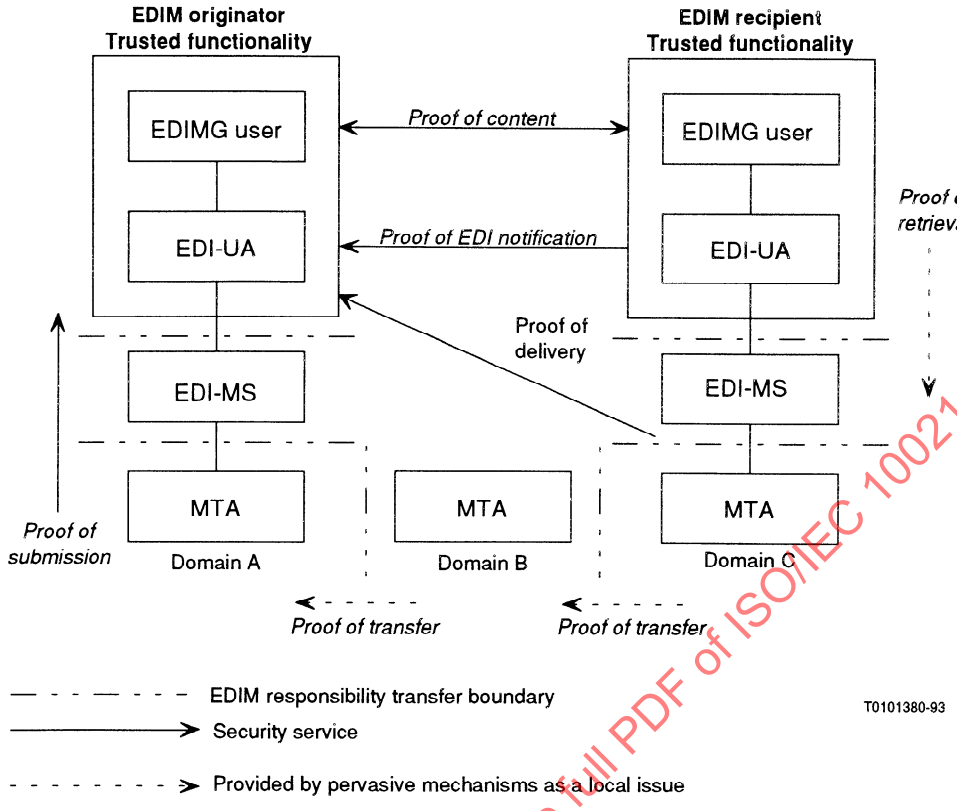


Figure C-1 – EDIM Responsibility transfer

"Non-repudiation/proof of transfer" counters the vulnerability of repudiation of responsibility between MTA and/or management domains. EDIMG environments may provide such a service using additional pervasive mechanisms, such as security logs and archives within MTA and/or MTS boundaries. Such pervasive mechanisms provide a "secure MT audit trail" to record the message details and trace information.

"Non-repudiation/proof of retrieval" counters the vulnerability of repudiation of responsibility of a message between a UA and an MS. EDIMG environments may provide such a service using additional pervasive mechanisms, such as security logs and archives within EDI-MSs. Such pervasive mechanisms provide a "secure EDI-MS audit trail" to record EDIMG user actions in the EDI message store.

"Non-repudiation/proof of EDI notification" counters the vulnerability of repudiation of an EDI notification EDI-UA to EDI-UA. This service is specific to EDIMG and a complete solution is included in this part of ISO/IEC 10021. This vulnerability may be especially relevant in the case of EDI forwarding, redirection, etc, in addition to the scenario of delivery to an untrusted EDI message store.

Two mechanisms have been defined for non-repudiation of EDI notifications, the first uses the trusted EDI notification as described above, the second uses an external notary systems. Only the trusted EDI notification was fully defined in this part of ISO/IEC 10021. External notary systems may be the subject of future standardization.

"Non-repudiation/proof of content" counters the vulnerability of manipulation of information by the EDIMG user after the message has been received by the EDI-UA. Although such vulnerability is outside the MHS environment, the MHS environment may provide assistance in terms of trusted return of content and notarization services. There are several ways this requirement may be supported, using the secure messaging environment based on the security services provided in 1992.